FM 6-02.71

NETWORK OPERATIONS

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 6-02.71

Headquarters
Department of the Army
Washington, DC

NETWORK OPERATIONS

Contents

Figures

Tables

Preface

FM 6-02.71 provides doctrine for the overall guidance and direction pertaining to the command and control of Army communications networks (voice, video, and data) and information services (collaboration, messaging, storage, mediation, etc.) throughout strategic, operational, and tactical levels. It describes the Army's portion of the Global Information Grid (hereafter referred to as LandWarNet), network operations goals and objectives, and the associated roles and responsibilities of applicable organizations, materiel, leadership, personnel, and facilities that must integrate LandWarNet standards, telecommunications, services, and applications for the purpose of enabling warfighters to conduct the information management and knowledge management tasks necessary to meet achieve information superiority and decision dominance.

The network operations construct is an integrated operational framework consisting of network management/enterprise systems management, information assurance/computer network defense, and information dissemination management/content staging. This manual provides a general functional understanding of each network operations component, along with an understanding of why the components must be integrated in order to meet overall objectives.

As stated, network operations are critical to the command and control of organizational communications networks and information services that enable commanders to use the network in order to shape and influence operations. Its principles allow for assured network and information system availability, assured information protection, and assured information delivery. The result is a horizontal fusion of information that flows to the right place, at the right time, and in the right format in order to attain information superiority and decision dominance over any adversary.

This publication has been prepared under the direction of the Commander, TRADOC. It sets forth doctrine to govern the activities and performance of the Army in reference to network operations and provides the doctrinal basis for establishing interoperability in a joint, interagency, multinational environment. It provides military guidance for the exercise of authority by commanders. With that stated, it is not the intent of this publication to restrict the authority of commanders from organizing the force and executing the mission in a manner they deem most appropriate to ensure unity of effort in the accomplishment of the overall objective.

The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of other publications, this publication will take precedence unless the Commander, TRADOC.

The proponent of this publication is the United States Army Signal Center. Send comments and recommendations on DA Form 2028 via e-mail to signal.doctrine@conus.army.mil or signal.doctrine@us.army.mil. Key your comments and recommendations to pages and lines of text to which they apply. Provide reasons for your comments to ensure understanding and proper evaluation.

Mailing address is Commander, United States Army Signal Center and Fort Gordon, ATTN: ATZH-IDC-CB (Doctrine Section), Building 29808, 506 Chamberlain Ave, Fort Gordon, GA 30905-5075.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1
Network Operations Overview

This chapter discusses the Global Information Grid (GIG), the Army's portion of the GIG – LandWarNet (LWN), and the integrated components of network operations (NETOPS) used to command and control LWN across strategic, operational, and tactical levels in support of commanders' information requirements. This chapter additionally discusses the functional services, critical capabilities, and effects enabled by each component. The chapter concludes by mentioning the principles associated with NETOPS, as well as the Army enterprise network infrastructure concept utilized to integrate network processes across full spectrum operations.

SECTION I – GLOBAL INFORMATION GRID

1-1. Joint Publication (JP) 6.0 defines the GIG as "the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for acquiring, processing, storing, transporting, controlling, and presenting information on demand to joint forces and support personnel." The GIG—

- Spans all services and components and includes all owned and leased computing systems, communications, software and applications, data, security services, and other information services necessary to achieve information superiority.
- Supports all Department of Defense (DOD), national security, and related intelligence community missions and functions (strategic, operational, tactical, and business).
- Extends capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites).
- Provides interfaces to multinational, coalition, non-DOD users, and systems as required.
- Integrates computing platforms, weapons systems, and sensors that exchange information through a globally interconnected network.

1-2. In concept, the GIG is very much like the Worldwide Web. It exists as a baseline capability and is comprised of information and information services residing on transporting infrastructures and segments. It is important to note that the GIG is a portion of cyberspace. The DOD definition of cyberspace is "the global domain consisting of interdependent networks of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers." The GIG, as the DOD's portion of cyberspace, interacts with and provides connections to national and global cyberspace, the national information infrastructure and global information infrastructure respectively. DOD's strategy is to create the cyberspace domain by integrating the seven components of the GIG (warrior, global applications, computing, communications, NETOPS, information management, and foundation as described in Figure 1-1) in order to enable joint forces to achieve information superiority, as well as in the future, allow them to conduct offensive cyberspace operations when necessary. Authorized users access the GIG and its services either through military or commercial communications or through a series of entry points, e.g., standardized tactical entry point (STEP) and teleport facilities. These points provide information transfer gateways as a means of forming a junction of space-based, aerial, and terrestrial networks and a connection for strategic or fixed assets and tactical or deployed users. It provides multiple connection paths between information users and information producers and enables effective and efficient information flow.

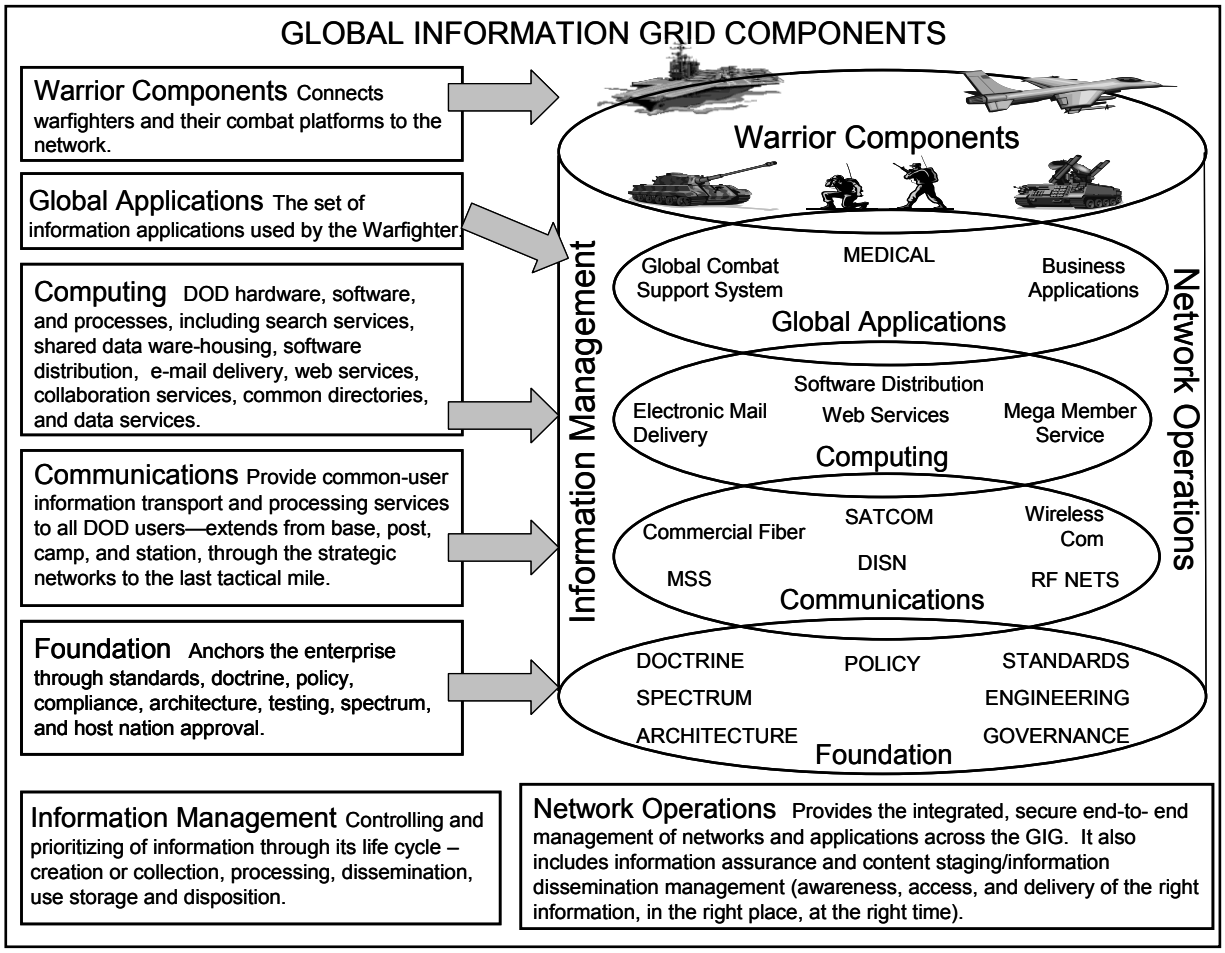

Figure 1-1. Global Information Grid

1-3. At the joint level, NETOPS is the operational construct implemented by the Commander, United States Strategic Command (CDRUSSTRATCOM) that provides the command and control and situation awareness (SA) required to operate and defend the GIG. NETOPS consists of GIG Enterprise Management, GIG Network Defense, and GIG Content Management. The purpose of NETOPS is to provide assured network and information system availability, assured information protection, and assured information delivery across strategic, operational, and tactical boundaries. The end result is a horizontal fusion across the GIG that ensures the right information flows to the right place, at the right time, and in the right format in order to achieve information superiority, and ultimately decision dominance. This supports the DOD's full spectrum of warfighting functions. NETOPS provides commanders the ability to harness the power of GIG and bring this power to the battlefield in order to shape and influence operations.

GLOBAL INFORMATION GRID GOVERNING BODIES

1-4. The governing bodies of the GIG are the Theater Joint Tactical Network Configuration Control Board (TJTNCCB), The Army Enterprise Infostructure Technical Configuration Control Board (CCB) and AENIA. These governing bodies have been empowered to approve, oversee, and enforce standards to ensure a shared view of the network through compatibility of equipment and software. The new registry/management tool for Information Technology Standard is the DOD Information System Registry.

JOINT TECHNICAL ARCHITECTURE-ARMY

1-5. The joint technical architecture-Army (JTA-A) requires all Army networks to use proven engineering criteria and modern communications equipment and technologies that are standard across the GIG. The use of standards ensures compatibility between US forces.

THEATER JOINT TACTICAL NETWORK CONFIGURATION CONTROL BOARD

1-6. The TJTNCCB governs tactical network and system equipment standards and capabilities. These standards lead to a common baseline of equipment and software throughout the tactical portion of the GIG. The Joint Tactical Switched Systems Network Management Configuration Control Board (JTSSNMCCB) grants exceptions and extensions under the following conditions:

- Nonstandard prototype capability fielding is an addition to the standard baseline fielding.
- Nonstandard capability is unique to a particular location and will be submitted to the TJTNCCB as an annex, but is not intended to become part of the standard configuration.
- Nonstandard capability is critical to a specific mission and not intended for use beyond the scope and time of the particular mission. If the nonstandard capability evolves into a recurring required capability, it must be submitted to the JTSSNMCCB for inclusion either as an annex or as a part of the standard configuration.

ARMY ENTERPRISE INFOSTRUCTURE TECHNICAL CONFIGURATION CONTROL BOARD

1-7. The Army Enterprise Infostructure Technical CCB was established by the CIO/G-6 to oversee the Army LWN Enterprise using standard change management to process the request for change submitted by Army organizations wanting to change their LWN infrastructure. NETCOM has the responsibility for configuration/change management.

1-8. NETCOM/9th SC(A) manages and maintains the Networthiness Regulatory Authority's network responsibilities and technical oversight over all organizations that operate and maintain portions of the LWN per Field Manual (FM) 3-0; AR 25-1, Para 2-2a(10); and AR 10-87.

LANDWARNET NETWORK OPERATIONS

Note. Global information grid enterprise management (GEM), global information grid network defense (GND), and global information grid content management (GCM) are joint and global network terms. These components at the LWN level are referred to as network management/enterprise systems management (NM/ESM), information assurance/computer network defense (IA/CND), and information dissemination management and content staging (IDM/CS) respectively. For the purpose of this field manual (FM), the terms refer to the same NETOPS processes at the GIG or LWN levels of the network. This construct aligns LWN NETOPS processes with the GIG NETOPS processes.

1-9. Inherent to the Joint mission, the Army's NETOPS mission is to provide command and control and situational awareness in order to operate and defend its portion of the GIG- the LWN. LWN encompasses the required standards, transport, services, and applications that enable warfighters to collect, process, store, transmit, and disseminate required information via the network from and to anywhere in the world. It enables the effective and efficient execution of all Army warfighting functions and facilitates the achievement of information superiority, which is necessary to make and execute accurate and timely decisions. It allows commanders to exercise command and control from anywhere in their area of operations. Unlike many missions that are deemed successful at a defined completion date, operating and defending LWN is perpetual and requires continual support to be successful.

1-10. LWN NETOPS is an integrated construct of three critical components (NM/ESM, IA/CND, and IDM/CS) that guide Signal entities in the installation, management, and protection of communications

networks and information services necessary to directly support operational forces. NETOPS provides users/systems, at all levels, with end-to-end network and information system availability, information protection, and timely information delivery.

1-11. An objective of the network-enabled management of information is to quickly get information to decision-makers, with adequate context, enabling them to make better decisions affecting the mission and to project their decisions forward to their forces for execution. If the decision maker is not getting the needed network-enabled services, the LWN NETOPS community must collaboratively determine who will take action and how information flow will be optimized. NETOPS personnel require a shared situational awareness/common operating picture; as well as the technologies, procedures, and collaborative organizational structures; to rapidly assess and respond to network and information system degradations, outages, or changes in operational priorities. All functions required to effectively support LWN operations will be holistically managed.

1-12. Information systems throughout areas of operations compete for the limited LWN access and capacity. NETOPS provides the means to operate and defend LWN transport, services, and applications in order to meet the commander's intent and priorities. This allows for better user/system support by—

- Identifying the information requirements (who, what, when, and where) of the user/system.
- Identifying the communications network and information service resources (hardware and software) required to fulfill user/system information requirements.
- Ensuring user/system access to the required communications networks and information services.
- Protecting the confidentiality, integrity, and availability of information and information systems with IA/CND measures coupled with the use of intelligence to enable threat-based risk management.
- Ensuring the establishment of information flows and information processing so that the right information is disseminated to the right place, at the right time, and in the right format.
- Identifying the resource requirements necessary to enable the wired, fiber, and wireless portion of the network.
- Ensuring that the allotment of resources is effectively utilized to efficiently maximize the bandwidth available to the user/system.

1-13. **The effectiveness of NETOPS** is measured in terms of availability and reliability of network enabled services, across all areas of interest, in adherence to required service levels. The method for service assurance in a network-enabled collaborative environment is to establish operational thresholds, compliance monitoring, and a clear understanding of the capabilities between providers and consumers through **service level agreements (SLAs)**. Proper instrumentation of the LWN enables monitoring of adherence to these SLAs, as well as enables timely decision making/execution, service prioritization, resource allocation, root cause, and mission impact assessment.

1-14. **The purpose of NETOPS is to provide** assured network and information system availability, assured information protection, and assured information delivery. These objectives are all required to achieve and sustain operational goals. Adhering to the NETOPS mission and performing the essential tasks associated with the three NETOPS components provides warfighters with the desired information effects. Integration of the NETOPS components must be performed at the strategic, operational, and tactical levels and across all warfighting functions. Thus, Signal entities must command and control the entire network within the operational area and be cognizant of the performance of those portions of the LWN outside of the operational area that affect the information requirements of the commander.

NETWORK OPERATIONS COMPONENTS AND EFFECTS

1-15. Assured network availability provides visibility and control over the network and information system resources. These resources are effectively managed and problems are anticipated and mitigated. Proactive measures are taken to ensure the uninterrupted availability and protection of the network and information system resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points.

1-16. Assured information protection provides protection for the information traversing networks and residing on information systems – from the time it is collected, stored, and processed until it is discovered, distributed, and utilized by the users, systems, and decision makers. Information protection is active or passive measures to protect and defend friendly information and information systems to ensure friendly access to timely, accurate, and relevant information while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Information protection comprises information assurance (IA), computer network defense (CND), and electronic protect capabilities (FM 3-0).

1-17. Assured information delivery provides information to users, systems, and decision makers in a timely manner. The networks are continuously monitored to ensure the information is transferred with the correct response time, throughput, availability, and performance that meet user/system needs.

1-18. NETOPS is the methodical integration of NM/ESM, IA/CND, and IDM/CS components' individual capabilities and the resultant synergy. In addition, NM/ESM, IA/CND, and IDM/CS are the Signal Regiment's core competencies. Figure 1-2 depicts and establishes a common understanding of the technical composition that must be considered to provide and sustain the effects of NETOPS. The center of the diagram illustrates the three NETOPS components, their relationships, and the desired effects once they are transformed into a tightly integrated NETOPS capability.

1-19. The three NETOPS critical components are discussed in the following sections.

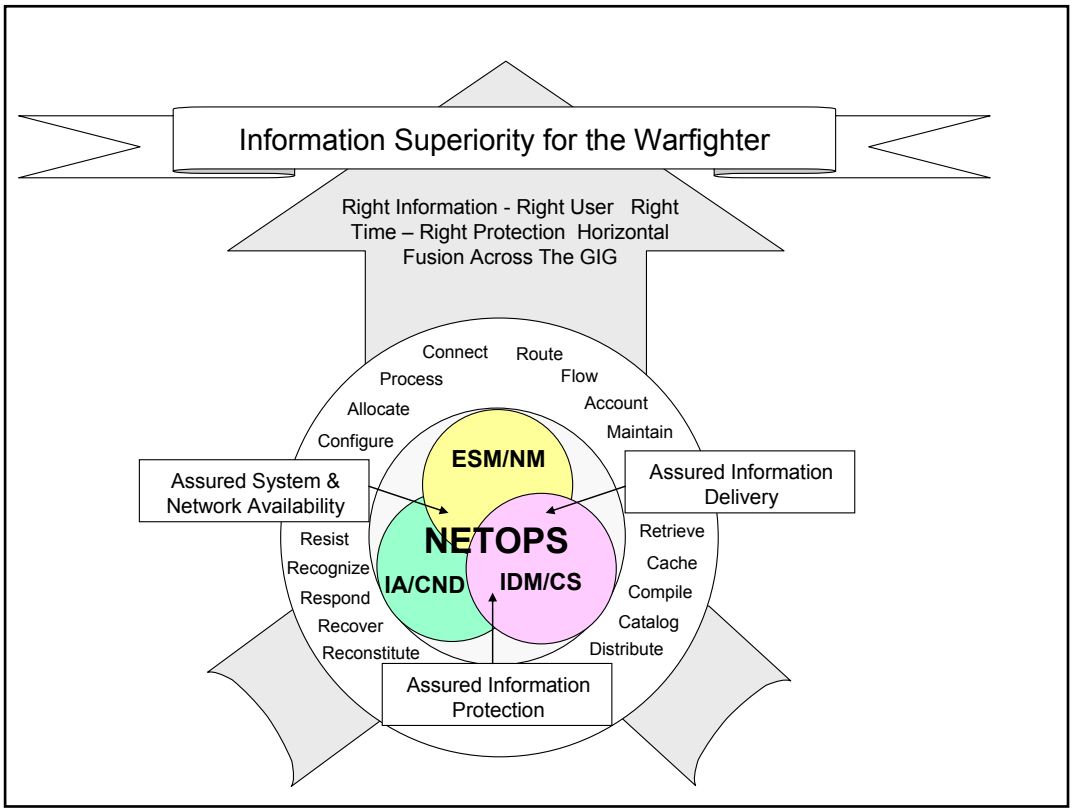

Figure 1-2. NETOPS components, effects, and objectives

NETWORK MANAGEMENT/ENTERPRISE SYSTEMS MANAGEMENT

1-20. NM/ESM is defined as the technologies, processes, and policies necessary to effectively and efficiently engineer, install, operate, manage, administer, optimize, and restore communications networks, information systems, and/or applicable applications that comprise the LWN. This essential component merges information technology (IT) services with the NETOPS critical capabilities.

1-21. Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems in order to provide the desired level of quality and guaranteed availability

1-22. Enterprise systems management refers to network-wide administration of distributed information systems through performance monitoring, configuration management (CM) and problem detection/resolution, ESM is strongly influenced by network management initiatives in telecommunications.

Functional Services

1-23. There are five major functional services within NM/ESM. These services foster the engineering, installation, operation, management, administration, optimization, and restoration of communications networks and information services technologies to ensure the effective and efficient operation, performance, availability, and security of information and information systems. These services must be employed at the strategic, operational, and tactical levels across all Army warfighting functions. The five services are—

- **Enterprise services availability** for end-user/systems applications and focuses on the accessibility, reachability, availability, performance, and responsiveness of enterprise service capabilities. An "enterprise" is described as a set of diverse, physically separated, but related, components that work together in order to achieve a functional objective. Enterprise services are those that offer collaborative, software distribution, messaging, discovery, storage, user/system assistance, and security functionality.
- **Systems availability** provides the day-to-day management of computer-based systems, elements of systems, and services to include software applications, operating systems, databases, and hosts of the end-users. System management comprises of all the measures necessary to ensure the effective and efficient operations of the LWN systems and elements of systems and services.
- **Network availability** provides the functionality of a network infrastructure with the desired level of quality and guaranteed service. Networks included within NM/ESM are located on all three tiers of communication (terrestrial, aerial, or satellite communications [SATCOM]), and they include: circuit-switched, packet-switched, and cell-switched networks utilizing wired, fiber, or wireless transport media. .
- **SATCOM availability** is the day-to-day operational management of all apportioned and non-apportioned SATCOM resources, to include appropriate support when disruption of service occurs; provides SATCOM system status; maintains situational awareness to include the organization's current and planned operations as well as space, control, and terminal segment asset and operational configuration management, satellite anomaly resolution and management, and SATCOM interference to the network.
- **Electromagnetic spectrum availability** involves the effective and efficient utilization of the electromagnetic spectrum including: international planning; frequency allotment; coordination with civilian and other government departments, agencies, military Services and components, and allies; frequency assignment, allotment, and approval; protection; frequency deconfliction; interference resolution; and coordination with electronic warfare activities. Spectrum management ensures that the combatant commanders (CCDRs) and subordinate commanders have cognizance of all spectrum management decisions that impact accomplishment of their missions (refer to FMI 6-02.70).

Critical Capabilities

1-24. NM/ESM involves several NETOPS critical capabilities associated with the IT services previously discussed. The critical capabilities for NM/ESM must be achieved at the strategic, operational, and tactical levels across all warfighting functions. The critical capabilities of NM/ESM are:

- Fault management is associated with failure of the network or information systems, which impacts connectivity and functionality. Fault management involves a five-step process of detecting faults, locating faults, restoring service, identifying the root cause of the fault, and establishing solutions so that similar faults do not occur in the future.

- Configuration management is used to discover the specifics of network and information system architectures and then developing configuration parameters. The parameters then guide the provisioning, deployment, and management of hardware and software resources.
- Accounting management assists in the effective and efficient allocation of internal and external resources to the warfighter. The goal is to identify true requirements based on monitoring network and system utilization. The end result is that the configuration of the network and information systems provides for the most effective and efficient use of current resources; as well as the data gathered during monitoring assists in the planning of future resources.
- Performance management is the monitoring and management of performance parameters related to networks and information systems. The purpose of networks and information systems is to transmit and process information; thus performance management is actually data traffic management. It involves data monitoring, problem isolation, performance tuning, analysis of statistical data for recognizing trends, and resource planning.
- Security management is both the technical and administrative considerations involved in securing access to the information being transmitted over the network or being processed/stored on information systems. Security management is the capability that integrates NM/ESM with IA/CND.

Enabled Effects

1-25. NM/ESM enables the effects of assured network and information system availability and assured information delivery. This is achieved by —

- Maintaining robust LWN capabilities in the face of component or system failure and adversarial attack.
- Configuring and allocating the LWN network and information system resources.
- Accounting for resource usage.
- Rapidly and flexibly deploying networked resources.
- Ensuring effective, efficient, and timely processing. As well as connectivity, routing, and information flow.
- Planning for increased network utilization.

INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE

1-26. IA/CND provides true end-to-end, defense-in-depth protection that ensures data confidentiality, integrity, and availability, as well as protection against unauthorized access.

1-27. IA is defined as measures that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and nonrepudiation. It considers both the technical and non-technical measures (such as risk management, personnel training, audits, business continuity/disaster recovery planning, etc.). Additionally IA holistically factors all incidents that occur through malicious or accidental activity by enemy or friendly entities. IA includes providing for restoration of information systems and information by incorporating protection, detection, and reaction capabilities.

1-28. CND is a sub-set of IA that provides defensive measures to protect and defend information, information systems, and networks from disruption, denial, degradation, or destruction. CND incorporates technical actions taken specifically to protect, monitor, analyze, detect, and respond to unauthorized, malicious activity.

Functional Services

1-29. The 10 functional services within IA/CND help to protect friendly information, networks, and information systems, while denying adversaries access to the same information, networks, and information systems. The 10 functional services of IA/CND are:

- **Access control** to information and information systems, which is influenced by the mechanisms that work together to create a secure environment that protects assets on the network. Access control provides the capability to specify what resources users can access and what actions users can perform.
- **Application security** provides security to software applications and software solution development, which is the environment where software is internally designed and developed. Some examples of application security solutions are software update service and patch management.
- **Business continuity and disaster recovery** provides preservation and recovery of information and network/information systems resources in the event of incidents that have the potential to interrupt normal operations.
- **Communications security** provides the principles, means, and methods of disguising voice, video, data, and imagery information to ensure confidentiality, integrity, authentication, and non-repudiation.
- **Risk analysis** identifies organization information assets, the threats and vulnerabilities against those assets, and the development of documentation and the implementation of policies, standards, procedures, and guidelines that relate to countermeasures.
- **Legal and regulatory compliance** enables the organization to meet the requirement for applicable individuals to be aware of and understand the IA/CND standards that must be met based on U.S., DOD, and Army laws and regulations. It additionally assists investigative efforts used to determine if defenses have been breached.
- **Development of IA/CND policies and procedures** specifically related to organizational personnel, hardware, software, and media. The capability identifies security guidelines for data/media, telecommunications equipment, and information systems. The capability additionally provides for the security activities required by users and Signal Regimental Soldiers. Examples of the required activities are log monitoring or analyzing audit trails.
- **Physical (environmental) security** encompasses protection techniques for the entire network facility, from the outside perimeter to the inside operational space, including all information system resources. Physical security provides measures to safeguard and protect network and information systems against damage, loss, and theft. Physical (environment) security provides for the determination and integration of site selection criteria related to network facilities and implements effective perimeter and interior security for those facilities. It additionally provides for the implementation of measures that enable adequate temperature, humidity, and fire controls.
- **Security in development and acquisition** provides the implementation of concepts, principles, structures, and standards used to acquire hardware and software resources in order to enforce various levels of confidentiality, integrity, and availability. The key is the integration of the common set of security criteria found in Army, DOD, and international standards – to include the trusted computing base and reference monitor concepts.
- **Telecommunications and network security** provide for the implementation of network architectures; transmission methods; transport formats; security measures to provide confidentiality, integrity, and availability; and authentication for transmission over private and public communications and media. Common solutions include intrusion detection/prevention systems, anti-virus solutions, web caches, and firewalls. Network security is achieved by engineering, installing, operating, and maintaining secure networks that incorporate cross domain solutions, remote access protocols, internet protocol security (IPSEC), virtual private networking (VPN) technologies, and access control lists.

Critical Capabilities

1-30. IA/CND involves several critical capabilities associated with the functional services previously addressed. The capabilities for IA/CND must be achieved at the strategic, operational, and tactical levels across all warfighting functions. IA/CND NETOPS critical capabilities include—

- **Protection** involves prior actions taken to counter vulnerabilities associated with information transport, processing, storage, and operational uses. Protection activities include emission security, communications security (COMSEC), computer security, information security, and critical infrastructure protection. In addition, protection addresses vulnerabilities presented by the physical (environmental) environment.
- **Monitoring** involves the examination of network and information systems to sense and assess abnormalities and the use of anomaly and intrusion detection systems (IDSs).
- **Detection** is instrumental to initiating system response and restoration actions. Timely detection, identification, and location of abnormalities include: attack, damage, unauthorized access attempts or modifications.
- **Analyzing** involves assessing pertinent information to determine indications and warnings, providing situational awareness, evaluating system status, identifying root cause, defining courses of action, and prioritizing response and recovery actions. These steps are taken in order to conduct the necessary reconfiguration of LWN assets and supporting elements.
- **Responding** requires that direct action is taken to mitigate the operational impact of an attack, damage, or other incapacitation of a network resource or information system. Response also includes restoration. This is the prioritized return of essential systems, elements of systems, or services to pre-event capability. CND response actions include defensive and restoration actions. Response actions are deliberate, authorized defensive measures or activities. These actions protect and defend systems and networks under attack or targeted for attack or exploitation by adversary systems and networks. Response actions extend defense in depth (DID) capabilities and increase the ability to withstand adversary attacks or exploitations. Objectives for using CND response actions include—
    - Strengthening the defensive posture and operational readiness.
    - Halting or minimizing attack and exploitation effects or damage.
    - Supporting rapid, complete attack, or exploitation characterization.

Enabled Effects

1-31. IA/CND enables the effects of assured information protection, and assured network and system availability. This is achieved by—

- Instituting agile capabilities (firewalls, password protect, intrusion detection, etc) to resist adversarial attacks, through recognition of such attacks as they are initiated or progressing.
- Detecting and performing analysis of an anomaly or intrusion, providing all Network Operations and Security Centers and the joint task force-global network operations (JTF-GNO) with incident reports.
- Directing response actions in their portion of the LWN.
- Alerting others on the LWN of incident local status to correct the intrusion.
- Certifying, accrediting and reporting on all networks, peripherals, and edge devices in their portion of the LWN in addition to enforcing information security.
- Conducting security readiness reviews and vulnerability analysis assessments of subordinate units for compliance with communications tasking orders, Information Assurance Vulnerability Managers (IAVMs), and reporting compliance to higher.
- Ensuring compliance of LWN management and defense training, awareness, and certification programs per established policies and directives.
- Developing and deconflicting local contingency plans to defend against malicious activity and providing copies to higher.

- Conducting risk assessments of networks.
- Sharing IA/CND information in accordance with (IAW) formal agreements and national disclosure policies except where limited by law, policy, or security classification.
- Providing reports as tasked.
- Developing and maintaining remediation, mitigation, and reconstitution plans for critical infrastructure protection criteria.

INFORMATION DISSEMINATION AND CONTENT STAGING

1-32. IDM/CS is defined as the technologies, techniques, processes, policies, and procedures necessary to technically provide warfighters awareness of relevant, accurate information; automated access to newly revealed or recurring information; and timely, efficient and assured technical delivery of information in a usable format. As IDM/CS becomes more mature, the complete complement of its services will be available for use by all authorized users/systems as a network-enabled service.

1-33. IDM enables warfighters to perform network-enabled information management tasks and seeks to achieve the dissemination of the right information, to the right place, at the right time, and in a usable format.

1-34. CS is a technique by which information is compiled, cataloged, and cached.

Functional Services

1-35. The functional services provided by IDM/CS are messaging, discovery, mediation, collaboration, storage, and user assistance in relation to voice, video, data, and imagery content. These core services are envisioned to be enterprise wide services used by the entire Army to ensure information is available to all authorized users. The LWN enterprise service effort and the network-enabled enterprise services program will deliver these core services. The core services are further described as:

- **Messaging** enables warfighters to exchange information among users and systems utilizing the network. Messaging examples include email, DOD unique message formats, message-oriented middleware, instant messaging, and alerts. Information that is received in the area of responsibility (AOR) by the information manager is delivered using the CS delivery service.
- **Discovery** enables warfighters to discover information content or services that exploit unique descriptions stored in directories, registries, and catalogs. An example of a discovery service is a search engine.
- **Mediation** enables system interoperability by processing data so that it is translated, aggregated, fused, or integrated with other data.
- **Collaboration** provides the ability for warfighters to work together and jointly use selected capabilities. Examples of collaboration services are chat, on-line meetings, and work group applications.
- **Storage** provides the physical and virtual hosting of data on the network with varying degrees of persistence, such as archiving, continuity of operations, and content staging. Information regarding storage locations may be listed in unit standing operating procedures (SOPs) or operations orders (OPORDs).
- **User Assistance** provides centralized, automated access to lessons learned information that reduces the effort required to perform manpower intensive tasks.

Critical Capabilities

1-36. IDM/CS involves several critical capabilities associated with the functional services previously addressed. The capabilities for IDM/CS must be achieved at the strategic, operational, and tactical levels across all warfighting functions. The IDM/CS NETOPS critical capabilities are:

- **Collection of information** describes acquiring data based on information requirements.
- **Processing of information** describes the act of translating data via an established and usually routine set of procedures to convert it from one form to another.
- **Storage of information** describes the recording of information to any medium residing on the network.
- **Transmission of information** describes the conveyance of information from one place to another based on a prescribed information flow.
- **Display of information** describes the visual presentation of information, data, or knowledge collected.
- **Dissemination of information** involves automated mechanisms that ensure collected and processed information is transmitted to the right person in a timely manner.

Enabled Effects

1-37. IDM/CS enables the effects of assured information delivery and assured information protection. This is achieved by—

- Retrieving critical information from information systems within the information environment that directly contribute to situational awareness, collaboration, and decision-making by the warfighter.
- Compiling the information retrieved in order for it to be processed and stored until needed.
- Caching the compiled information in a secure system IAW applicable regulations and policies.
- Cataloging the cached information in order to facilitate warfighter future search and discovery of required information.
- Distributing critical information to the warfighter or information system in order to gain situational awareness, conduct collaboration, or execute decisions.

SECTION II – NETWORK OPERATIONS PRINCIPLES

1-38. NETOPS principles allow for active involvement, coordination, status sharing, and cooperation of service providers for an open view of networks and information systems throughout the LWN. The following principles govern developing and implementing NETOPS.

SHARED NETWORK MANAGEMENT CONTROL

1-39. The components of the LWN are controlled by multiple organizations that provide network services to the functional user. These different organizations accomplish end-to-end management of a network by sharing information related to their assets and collaborating on problem resolution and service provisioning issues. Network service providers must know the status of major components of networks and information systems as well as their overall performance. Network operations and security centers (NOSCs) provide near- and real-time statuses. Information sharing should not imply sharing of control responsibilities beyond what is necessary to manage the network.

ASSURANCE AND PROTECTION OF INFORMATION

1-40. A greater reliance on information to plan operations, deploy forces, and execute missions has placed increased emphasis on assuring and protecting information. Mission accomplishment depends on protecting and defending information and information systems from destruction, disruption, corruption, intrusion, and exploitation. Protection and defense of data and voice networks and information systems is accomplished through aggressive application of IA measures, CND, CND response action, critical infrastructure protection, and NETOPS force protection in defense of the LWN.

DISSEMINATION OF INFORMATION

1-41. Managing and protecting networks and information systems does not alone ensure that relevant information is being disseminated to the intended user. A major component of NETOPS is the management of the delivery of relevant and accurate information, to the appropriate user, in an efficient manner, and in the proper format.

INTEGRATED ARCHITECTURE

1-42. As our Army strives to achieve the objectives of joint net-centric warfare, Army transformation, and a modularized force, we must have an integrated enterprise-wide NETOPS architecture to effectively manage both battlefield and business network environments across the joint operating spectrum. The Army Enterprise Network Operations Integrated Architecture (AENIA) is a top-to-bottom enterprise vision, vice a specific program of record architecture that will evolve as the Army's transformation and modularity concepts, doctrine, architecture and organizations mature.

ARMY ENTERPRISE NETOPS INTEGRATED ARCHITECTURE

1-43. The AENIA is the baseline LWN enterprise NETOPS architecture for the Army's Chief Information Officer (CIO)/G-6 Policy Memorandum, 24 Apr 06. It was developed by NETCOM and is under the oversight of the CIO/G-6 as one of five architectures which collectively comprise the Army Knowledge Enterprise Architecture established per Army Regulation (AR) 25-1. The AENIA is based on DOD, joint, Army, installation, and industry "Best Business Practices" (Information Technology Infrastructure Library®) and supports the Army's IT Portfolio Management mandate.

1-44. The AENIA describes a standardized set of NETOPS capabilities for the LWN. It defines the organizations, roles, activities, and systems necessary to operate, manage, and defend the flow of information in the enterprise information environment. The NETOPS capabilities addressed within the AENIA v5.0 includes:

- Internet Protocol (IP)-based transport management focusing on securely operating, managing, and maintaining firewalls, IP network management systems/applications, layer-2 switches, layer-4 switches, network intrusion detection devices, network intrusion prevention devices, routers, Voice over Internet Protocol (VOIP) systems/applications, Virtual Private Networks (VPNs), and wireless IP network systems. ***Note***: these generic network devices/systems may actually be combined as modules/components within a single system, cabinet, or device, as is the case with current Top Layer Architecture-Redesign 2 stacks.
- Computing platform management focusing on securely operating, managing, and maintaining anti-malware (anti-virus/spyware/adware) systems, backup and recovery systems, host IDSs, host intrusion prevention systems (IPSs), network attached storage devices, secure configuration remediation/patch management systems, storage area network systems, computer/server management systems/applications, data security at rest, and host-based security systems. The managed devices and management applications may also be combined as modules/components within a larger single system, cabinet, or application, as is the case with host-based security system; the AENIA requirements still apply.
- Security management focusing on securely operating, managing, and maintaining; IAVM compliance managers, IP network vulnerability scanners, security information management systems/applications, cryptographic systems, identity management systems/applications, public key infrastructure (PKI) systems, remote access systems, high assurance IP encryption systems, IP network policy-based servers/systems/applications, secure socket layer accelerator systems, network access control, and trusted platform module.
- Enterprise support focusing on providing the Army enterprise infostructure-repository, IP capacity and availability monitoring, help desk/customer relationship management/CM, NETOPS situation awareness, frequency assignment, and service level management.

- Enterprise services and applications management—focusing on securely operating, managing, and maintaining collaboration services, electronic-mail (e-mail) services, Lightweight Directory Access Protocol//X.500 services, Active Directory (AD) services (Refer to Appendix A for a detailed discussion of AD management), databases, meta-directory systems/applications/services, and organizational messaging services (the Defense Message System-Army).

Chapter 2

Network Operations Components

This chapter more thoroughly addresses the NM/ESM, IA/CND, and IDM/CS components of NETOPS. It describes the activities, responsibilities, associated functions, and tasks that must be accomplished to effectively and efficiently use the networks, systems, and resources that contribute to the Army's communications systems operation support mission.

SECTION I - ENTERPRISE SYSTEMS MANAGEMENT/NETWORK MANAGEMENT

2-1. The specific management requirements vary depending on the echelon of the systems and networks. This section will guide network managers during the activities, functions, and tasks performed at the strategic, theater, and tactical levels of NM/ESM.

2-2. The role of NM/ESM is to coordinate, manage, and control the installation and the operations and maintenance of networks and systems to meet user requirements. This objective requires performing a set of activities, functions, and tasks necessary to control the network's topology, maintain its operational capability, optimize its performance, and account for its usage.

OBJECTIVE

2-3. The NM/ESM mission provides network control for all Army communications systems operation and interaction with other services for various NM/ESM operations in joint networks. NM/ESM directs the allocation of responsibilities among Army and joint organizations. The Army's NETOPS managers perform NM/ESM at the strategic, theater, and tactical military operations levels. Specific functions and tasks may vary depending on the mission and capabilities of the organization. There is, however, a common set of activities that NETOPS managers perform for effective and efficient NM/ESM.

ACTIVITIES

2-4. The activities for the operation, management, and control of information networks and systems are performed consistently at NOSCs from the sustaining base to the theater tactical signal units (numbered Army, corps, and division) as well as to the brigade combat team (BCT) and battalion. These activities occur during the predeployment, deployment, and redeployment stages of an operation. NM/ESM is broken down into seven activities. Each activity represents a different step in the NM/ESM cycle. Network and information systems management resources are identified for each activity to create a manageable NM/ESM. Many of the activities required for NM/ESM are also necessary for the execution of general NETOPS. The seven activities are—

- Operational control and management.
- Service delivery.
- Service support.
- Mission planning.
- Capability design and engineering.

- Logistics.
- Administration.

2-5. Specific functions and associated tasks are accomplished within each activity of NM/ESM, whether it applies to user-owned, -operated, and -managed information systems or to voice and data networks provided by communications networks and information services support elements. A distinct separation exists between networks and their management and user information equipment operation and its management.

2-6. The user drives the NM/ESM activities and directly interfaces in three areas: operational control and management, service delivery, and service support. A user request for information support services initiates the cycle and is supported through the operational control and management activity. The NM/ESM cycle ends when network managers perform the service support activities that provide customer service and performance analysis of the user's needs. The various control centers perform the remaining activities to provide continuous network and information system support to the user.

2-7. Mission planning and capability design and engineering are centralized activities that design the networks to meet the user's service requirements. Logistics support is required for maintenance on existing services and procurement of equipment to meet new service requirements. The following paragraphs define NM/ESM activities and the associated functions and tasks.

Note. Refer to Chapter 5 for a detailed description of the activities required for NM/ESM and the execution of general NETOPS.

OPERATIONAL CONTROL AND MANAGEMENT

2-8. Network managers perform service provisioning to add, delete, or change network and information system services available to the user. Operational control and management covers the non-engineering tasks associated with providing users access to the requested services. Services may be of a global nature, such as the GIG long-haul capability controlled and managed by the Global Network Operations Support Center (GNSC). Services may also be the direct user services provided by a network manager at a NOSC and at the theater (numbered Army, corps, and division) or BCT tactical level of operations. Operational control and management involves—

- Configuration change implementation.
- Sub-element installation.
- Service modification verification.
- Configuration of end-user equipment.

SERVICE DELIVERY

2-9. Service delivery is the activity that directly interfaces with the user to monitor satisfaction with the service provided by the network or information systems components. Service delivery looks at what services the user requires of the provider in order to provide adequate support to the Army mission area. The service delivery management activities involve—

- Service level management.
- Financial management for IT services.
- Capacity management.
- IT service continuity management.
- Availability management.

SERVICE SUPPORT

2-10. Service support is the core NM/ESM activity that provides the monitoring and control to keep the network and systems operating and providing quality service. The service support targets network and systems operations and management. NETOPS managers perform this activity during the operational stages of the network. Service support involves—

- Service desk.
- Incident management.
- Problem management.
- CM.
- Change management.
- Release management.

MISSION PLANNING

2-11. The mission planning activity assesses user requirements and develops the schedule and resources to meet the requirements. It consists of functions that deal with the current, short-term (less than 2 years), and long-term (2–20 years) planning requirements. The mission planning activity ensures changes in requirements for services are collected, analyzed, prioritized, cost assessed, and scheduled for implementation. The ultimate goal of mission planning is to ensure that resources are available to meet current and emerging short-term and long-term requirements, and that proposed implementations conform to follow-on short- and long-term objectives. The mission planning activity involves—

- Analysis of user requirements.
- Technology assessment.
- Architecture definition.
- Services planning and programming.
- Sub-system definition and funding.
- Cost benefits analysis.
- Performance objectives establishment.
- Contingency and restoration planning.
- Capacity planning.
- System planning.
- Integration planning.
- Security planning.
- Frequency assignment.
- SATCOM management.

CAPABILITY DESIGN AND ENGINEERING

2-12. The capability design and engineering activity tailors network and information system resources to meet user service requirements. Capability design and engineering bases network and systems design requirements on planning direction that relates to capacity allocation and new services for implementation. Capability design and engineering is required from the strategic LWN level of NM/ESM, down to the theater (numbered Army, corps, and division) tactical NM/ESM performed by a theater network operations and security center (TNOSC). The capability design and engineering activity involves—

- Planning assistance to users.
- Network and systems design.
- Security design.
- Facility and equipment design.
- Integration of operations, facilities, and equipment.

- Technical documentation.
- Equipment and services specification.
- Implementation design and procedures development.
- Hardware and software development.
- Information systems support and development.
- Frequency assignment.

LOGISTICS

2-13. The logistics activity provides for the logistical support of the network and systems. Logistics includes procurement, handling, storage, packaging, distribution, maintenance, and replacement of materiel such as spare or repair parts and consumable items. Logistics activities involve—

- Corrective maintenance.
- Requisition processing.
- Equipment inventory management.
- Stockage.
- Property accountability.

ADMINISTRATION

2-14. The administration activity is associated with budgeting, training, procurement, staffing, and other business-related functions. Network managers perform these functions primarily at the strategic sustaining-base level and at theater bases, posts, camps, and stations. They also perform some of these functions to a lesser degree at all levels of NM/ESM. The administration activities involve—

- Training management.
- Program and budget management.
- Procurement.
- Staffing management.
- Chargeback.
- Special services.

SECTION II - INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE

OVERVIEW

2-15. Army commanders rely on information support to plan operations, deploy forces, and execute missions. By protecting the flow of information from attacks, intrusions, and interruptions, the commander can be assured of gaining and maintaining information superiority.

2-16. IA is the defensive component of information operations (IO) that with concurrent use of validated intelligence defining the threat enables the availability, integrity, authentication, confidentiality, and non-repudiation of friendly information and information systems in the information environment that is now a component of the operational environment. IA provides a DID that protects the LWN against exploitation, degradation, and denial of service. The DID incorporates vigorous protection, detection, reaction, and restoration capabilities. This incorporation allows for effective defensive measures and timely restoration of debilitated networks and information systems.

2-17. IA capabilities reside in depth throughout the LWN. Network and information system managers must actively monitor and evaluate the effectiveness of the IA systems used in their AOR. They must maintain an awareness of the overall network status, incident reporting, and network management processes to integrate IA into the NETOPS activities, functions, and tasks. IA-trained personnel must be integrated into the Army

NOSCs at all echelons. This placement ensures the expertise to quickly determine the cause of and take appropriate action in response to IA issues as they affect the LWN.

2-18. IA encompasses a diverse field of network and information systems security disciplines. The Army Information Assurance Program (AIAP) focuses the Army's efforts to secure information and its associated systems and resources. It provides a unified approach to protecting classified and sensitive information by using the risk management approach for implementing security safeguards. The AIAP is not limited to information security; it covers other aspects of security such as COMSEC, emission security, operations security (OPSEC), physical security, personnel security, and industrial security.

2-19. Commanders at all levels use the DID strategy to secure Army information and information systems against the full spectrum of capabilities of adversaries operating in the information environment and identified in paragraph 2-27, below. The interactive nature of the Army's technical networks and information systems using the publicly available Internet in light of these threats makes them vulnerable to intrusions and disruptions.

2-20. The DID strategy protects networks and information systems through a layered series of protective perimeters; enhanced protect, detect, and react capabilities; and a supporting IA infrastructure. It is a long-term, dynamic strategy that incorporates IA/CND tools and policy enforcement, and it uses current and evolving technology, policies, procedures, and trained, knowledgeable people. The strategy is flexible and adjusts to changes in technology that may pose new attack threats or offer new protection capabilities.

2-21. Commanders must develop comprehensive protection measures in anticipation of how an adversary may use elements of attack and intrusions to disrupt systems and networks. These measures keep in mind the guiding principles of the DID strategy, including risk management, vulnerability assessment, levels of concern and protection, and the capability to detect and react to attacks and intrusions.

INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE FUNDAMENTAL ATTRIBUTES

2-22. The IA/CND mission essential task ensures the fundamental attributes of availability, authentication, confidentiality, integrity and non-repudiation of friendly information and information systems while denying adversaries access to the same information and information systems. The fundamental attributes are—

- **Availability**. Actions taken to allow the timely, reliable access to data and information services for authorized users.
- **Authentication**. A security measure designed to establish the validity of a transmission, message, originator, or as a means of verifying an individual's authorization to access specific categories of information.
- **Confidentiality**. Actions taken that assure information is not disclosed to unauthorized individuals, processes, or devices.
- **Integrity**. Assuring the quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is interpreted more narrowly to protect against unauthorized modification or the destruction of information.
- **Non-repudiation**. Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity in order to create a record of the parties that processed the data.

2-23. IA/CND incorporates those actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. IA incorporates protection, detection, and response capabilities while providing for restoration of information systems. It provides end-to-end protection to ensure data quality and protection against unauthorized access and inadvertent damage or modification. CND activity employs IA protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information.

2-24. CND response actions include defensive and restoration actions. CND response actions are deliberate, authorized defensive measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems and networks. CND response actions extend DOD's layered DID capabilities and increase DOD's ability to withstand adversary attacks. Objectives for using CND response actions include:

- Strengthening DOD's defensive posture and operational readiness.
- Halting or minimizing attack effects or damage.
- Supporting rapid, complete attack characterization.

2-25. IA and CND are focused on assured information protection and assured network and information system availability. The objectives of this focus are achieved by—

- Instituting agile capabilities (firewalls, password protect, intrusion detection, etc) to resist adversarial attacks through recognition of the attacks as they are initiated or are progressing.
- Efficient and effective response actions to counter the attack, and safely and securely recover from such attacks.
- Reconstituting capabilities from reserve or reallocated assets when original capabilities are destroyed.
- Maintaining correlation activities between user elements to ascertain hostile IA/CND events from other system outages or degradations.

RISK MANAGEMENT

2-26. A comprehensive risk management program is the most effective way to protect a network or information system. Risk management consists of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. The objective of risk management is to achieve the most effective safeguards against threats of both intentional and unintentional intrusions into a network or system. Intentional intrusions are planned attacks against information resources and must be protected by an effective DID. Risk management also includes identifying network and information system vulnerabilities created by weaknesses in design, ineffective security procedures, or faulty internal controls that are susceptible to exploitation by authorized or unauthorized users. The following paragraphs discuss the aspects of risk management. (Refer to FM 5-19 for additional information on risk management.)

THREAT

2-27. Threats to the GIG and LWN are genuine, world-wide in origin, technically multifaceted and growing. They come from individuals and groups motivated my military, political, cultural, ethnic, religious, personal, or industrial gain. These types of threats are categorized by the Committee on National Security Systems Instruction No. 4009 as incidents (assessed occurrence having actual or potential adverse effects on an information system, or events occurrences, not yet assessed, that may affect the performance of an information system). According to FM 3-13, the capabilities of adversaries operating in the information environment are:

- **First level**: lone or small groups of amateurs using common hacker tools and techniques in an unsophisticated manner without significant support.
- **Second level**: individuals or small groups supported by commercial business entities, criminal syndicates, or other transnational groups using common hacker tools in a sophisticated manner. This level of adversary includes terrorists and non-governmental terrorist organizations. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft.
- **Third level**: individuals or small groups supported by state-sponsored institutions (military or civilian) and significant resources, using sophisticated tools. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft.
- **Fourth level**: state-sponsored offensive IO, especially computer network attacks, using state-of-the-art tools and covert techniques conducted in coordination with (ICW) military operations.

2-28. These events and incidents (both initiated by potential or actual adversaries or by Army users or administrators as a result of carelessness or non-compliance) are identified by the IA and CND communities into categories that include:

- **Category 1**: root level intrusion (incident) unauthorized privileged access (administrative or root access to a DOD system).
- **Category 2**: user-level intrusion (incident) unauthorized non-privileged access (user-level permissions) to a DOD system.
- **Category 3**: unsuccessful activity attempt (event) attempt to gain unauthorized access to the system that is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (e.g., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized by as exploratory scanning.
- **Category 4**: denial of service (incident) activity that impairs, impedes, or halts normal functionality of a system or network.
- **Category 5**: non-compliance activity (event) activity that due to DOD actions (or non-actions) makes an IT system potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.).
- **Category 6**: reconnaissance (event) an activity (scan or probe) that seeks to identify a computer, an open port, an open service, or any combination thereof for later exploit.
- **Category 7**: malicious logic (incident) installation of malicious software (e.g., Trojan, backdoor, virus, or worm).

2-29. The globalization of network communications and the IT marketplace creates vulnerabilities due to increased access to the information infrastructure from points around the world and the uncertainties of the security of the IT supply chain. The global commercial supply chain provides adversaries with greater opportunities to manipulate information and communications technology products over the products life cycle…adversaries have greater access to our networks when (their) products or services are delivered. Threats against computers, network, and information systems vary by the level of hostility (peacetime, conflict, or war), technical capabilities and motivation of the perpetrator. Threats to the information systems and networks relied upon by strategic and tactical forces exist from various sources, and they exist on a continual basis.

2-30. Attacks and intrusions compromise missions, corrupt data, degrade networks and systems, and can destroy hardware and software applications. These results hamper the effectiveness of support forces and the supported Soldier.

Intentional Intrusion

2-31. Intentional intrusion into a network or system is a deliberate act. This act has proven to be one of the most challenging to protect against, detect, and react to. Examples of intentional intrusion include—

- Unauthorized users, such as attackers. Attackers are the source of most attacks against information systems in peacetime. They mostly target personal computers, but recently have targeted network communications, mainframes, and local area network (LAN) based computers.
- Trusted insiders with legitimate access to a system. They pose one of the most difficult threats to defend. Whether recruited or self-motivated, insiders can access systems normally protected against attack. While insiders can attack at almost any time, a system is most vulnerable during the design, production, transport, and maintenance stage.
- Terrorist groups who have access to commercial information systems (including the Internet). They may obtain unauthorized access to an information network or direct attacks against the infrastructure (bombing). Terrorists use computer bulletin boards and Internet systems to pass intelligence and technical data across international borders. These organized groups pose a serious threat to the information infrastructure and national security of the US.

- Non-state groups, such as drug cartels and social activists. Taking advantage of the information age, they can acquire (at low cost) the capabilities to strike at their foes' commercial, security, and communications infrastructures. Moreover, they can strike from a distance with impunity.
- Foreign intelligence services that are active during peace and conflict and take advantage of the anonymity offered by the computer, bulletin boards, and the Internet. They hide organized collection or disruption activities behind the facade of unorganized attackers. Their primary targets are often commercial, scientific, and university networks. They may also directly attack military and government networks and systems.
- Opposing militaries or political opponents. While the adversary's activities are more traditionally associated with open conflict or war, opposing militaries or political opponents may invade US computer and telecommunications networks during peacetime. Such strikes help frame the situation to their advantage preceding the onset of hostilities. Adversaries may also try to manipulate the news media and public opinion to their advantage.

ATTACKS

2-32. An intentional intrusion is an attack against computers or information systems. Some attacks have a delayed effect and others are immediate. Both the delayed and immediate attacks corrupt databases and controlling programs, and may degrade or physically destroy the system attacked. Timely attack detection is essential to initiating network restoration and network intrusion response capabilities. The following paragraphs discuss types of attacks.

2-33. Computer attacks generally aim at software or data contained in either end-user or network infrastructure computers. Adversaries aim at unobtrusively accessing information, modifying software and data, or totally destroying software and data. These activities can target individual computers or a number of computers connected to a LAN or wide area network (WAN). Computer attacks may take place during routine tactical operations and may be multifaceted to disrupt major military missions. These attacks can also take place during wartime and peacetime. Attacks can be part of a major nation-state effort to cripple the US national information infrastructure. They can also come from mischievous or vengeful insiders, criminals, political dissidents, terrorists, and foreign espionage agents.

2-34. Malicious computer attacks can be intentionally designed to unleash computer viruses, trigger future attacks, or install software programs that compromise or damage information and systems. They may also involve unauthorized copying of files, directly deleting files, or introducing malicious software or data. Malicious software generally consists of executable software codes secretly introduced into a computer and includes viruses, Trojan horses, trap-doors, and worms. Malicious data insertion, sometimes termed “spoofing,” misleads a user or disrupts systems operation. For example, an attack disrupts a packet data network by introducing false routing table data into one or more routers. An attacker who denies service or corrupt data on a wide scale may weaken user confidence in the information they receive by corrupting or sending false data.

2-35. Physical attacks generally deny service and involve destruction, damage, overrun, or capture of the systems components. This may include end-user computers, communications devices, and network infrastructure components. A physical attack involves the overrun and capture of computer equipment that allows the adversary to employ a computer attack. Another form of physical attack is theft of items, such as cryptographic keys or passwords. This is a major concern since these items can support subsequent electronic or computer attacks.

2-36. Electronic attacks focus on specific or multiple targets within a wide area. Attacks against communications links include the following two types of signal intelligence operations: signal intercept and analysis to compromised data and emitter direction findings, and geo-location to support signal analysis and physical attacks. “Jamming” is another attack against communications links. Jamming corrupts data and may cause denial of service to users. For example, the jamming of communications links supporting global positioning system users is a specific concern.

VULNERABILITIES

2-37. The information age has enabled the Army to use information as an element of combat power. Supporting crises and contingency operations require the rapid expansion of IO capabilities beyond their normal peacetime limits. Deploying forces require secure video, database connectivity, and broadcast and receive capabilities for reach operations access to intelligence, logistics, and other essential support data. Successful conduct of operations requires access to information available outside the operational area. Information infrastructures no longer parallel traditional command lines. Soldiers need frequent, instant, and reliable access to information in the continental United States (CONUS) and outside the continental United States (OCONUS). The Soldiers' mobility capabilities and force sustainment requirements depend on commercial reach operations infrastructures that include international telecommunications and the public switched networks.

2-38. This increased reliance on reach operations information capabilities by the Soldier has created vulnerabilities to attack from various sources. Networks and information systems are vulnerable to attack from adversaries who can quickly take advantage of weaknesses in design, ineffective or lax security procedures, or insufficient internal controls. An adversary who may not be a technological equivalent could initiate a covert or overt attack by using inexpensive, commercial off-the-shelf products and attacker tools obtained from the Internet. The attack can be from any location that has access to the Internet. Recent trends that have increased vulnerability include use of commercial services, commercial off-the-shelf hardware and software, the integration and consolidation of stovepipe systems, moving toward an open systems environment, and extensive interfacing with government, industry, and public networks. (Refer to AR 25-2 for specific examples of vulnerabilities.)

2-39. A vulnerability analysis should be conducted to assess the security status of networks and information systems. A vulnerability analysis should be conducted or requested at every organizational level. The analysis can ensure that the network or information systems security features are properly configured for optimum IA capabilities. Another critical component of an effective vulnerability analysis program is the periodic review of the IA tools in use to ensure that the latest version is installed. An effective program will identify unauthorized users and unauthorized use of the network or information system. Once unauthorized activity is identified and verified, established incident and vulnerability reporting procedures must be followed. The reporting procedures are outlined in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 and AR 25-2.

INFORMATION SYSTEMS SECURITY

2-40. IA programs within the Army must include the full range of security measures. Information systems security occurs only when a common set of technical procedures apply to all assets connected to the common-user LAN and throughout the WAN. Protection from intrusions into or via a WAN must begin with a cooperative information systems security effort between all of the services and the Defense Information Systems Agency (DISA). All security measures taken to detect, respond to, react to, and report attacks and intrusions will adhere to public laws, DOD directives, and ARs. System administrators and network managers are required to complete IA security and awareness certification training. Specific information regarding measures to reduce the threat, vulnerabilities, and risks will be covered for the information systems under their purview.

LEVEL OF CONCERN

2-41. All information systems will be assigned a level of concern rating based on the confidentiality, integrity, and availability of the information processed, stored, or transmitted. The level of concern rating for each of these areas can be basic, medium, or high. The decision regarding the level of concern will be explicit for all systems. (Refer to AR 25-2 for more information on the level of concern rating process.)

PROTECTION LEVELS

2-42. Protection levels only apply to confidentiality requirements. Protection levels are based on the required clearance, formal access approval, and need-to-know of all direct and indirect users who receive information from the information systems without manual intervention and reliable human review. Protection levels indicate the implicit level of trust that is placed in the system's technical capabilities. The service providers and the users must cooperate to implement the required level of protection. The Soldier must have assurance that his information systems have the level of protection or trust required for a successful mission.

PROTECTION, DETECTION, AND REACTION CAPABILITIES

2-43. Information and network systems are critical to the military's ability to conduct operations. The Soldier's assurance that networks and information systems are defended adequately against attack requires the ability to—

- Protect the information that computer systems and data networks pass and store.
- Detect when an intrusion into the network or information system happens.
- React to contain the damage and repair the network or information system.

PROTECTION

2-44. Information protection is active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes (FM 3-0).

2-45. Information protection includes information assurance, computer network defense, and electronic protection. All three are interrelated.

- Information assurance consists of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (JP 3-13).
- Computer network defense consists of actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks (JP 6-0). Effective network defense assures Army computer networks' functionality. It detects and defeats intruders attempting to exploit Army information and information systems. Commanders and staffs remain aware of and account for information on regulated (Department of Defense) and nonregulated (Internet) networks. They analyze how information from these mediums affects their operation; they take action to mitigate the associated risks.
- Electronic protection is that division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-13.1).

2-46. Information protection applies to any medium and form including hard copy, electronic, magnetic, video, imagery, voice, telegraph, computer, and human. Information protection involves determining the appropriate security measures based on the value of information protected. The protection measures should reflect the changing value of the information that pertains to each operational phase of any given mission. Ensuring the protection of information is the responsibility of leaders, information producers, processors, and users.

2-47. Continuity of operations (COOP), operations plans, and OPORDs specify the priorities of protection measures for network and information systems. The protection measures should consist of firewalls, IDSs, and software that harden these systems against intruders. Figure 2-1 is an example of the basic network and

information systems protection measures. Every effort must be made to improve the protection of information stored on US computers and that flows through the networks.

2-48. Army network and system managers must devise and implement comprehensive plans for using a full range of security means. The plans will include external and internal perimeter protection. External perimeter protection consists of COMSEC, router filtering, access control lists (ACL), security guards, and physical isolation serving as a barrier to outside networks such as the Non-Secure Internet Protocol Router Network (NIPRNET). Internal perimeter protection consists of firewalls and router filtering. These serve as barriers between echelons of interconnected networks and information systems. Internal COMSEC barriers are also required. Local workstation protection consists of individual access controls, configuration audit capability, protection and intrusion detection tools, and security procedures.

2-49. Other considerations that must be addressed when protecting vital networks and information systems include—

- Developing comprehensive training programs. Programs should instill IA intrusion and detection doctrine, and operational procedures in all members of the command.
- Developing vigorous programs for sharing results of red team and vulnerability assessments.
- Programs that have a standard practice at the appropriate levels of information flow and—
    - Ensure intrusion protection and detection systems are employed at all levels of network management.
    - Train to protect against, detect, react to, and restore from intrusions should become a common task.

2-50. Other initiatives to enhance the architecture and limit intrusions into the NIPRNET are underway. These initiatives include routing communications through a limited number of gateways and closing access to networks through other connection points around the globe (thus easing monitoring tasks and responsibilities), and upgrading firewalls and IDS devices to help prevent unauthorized entries.

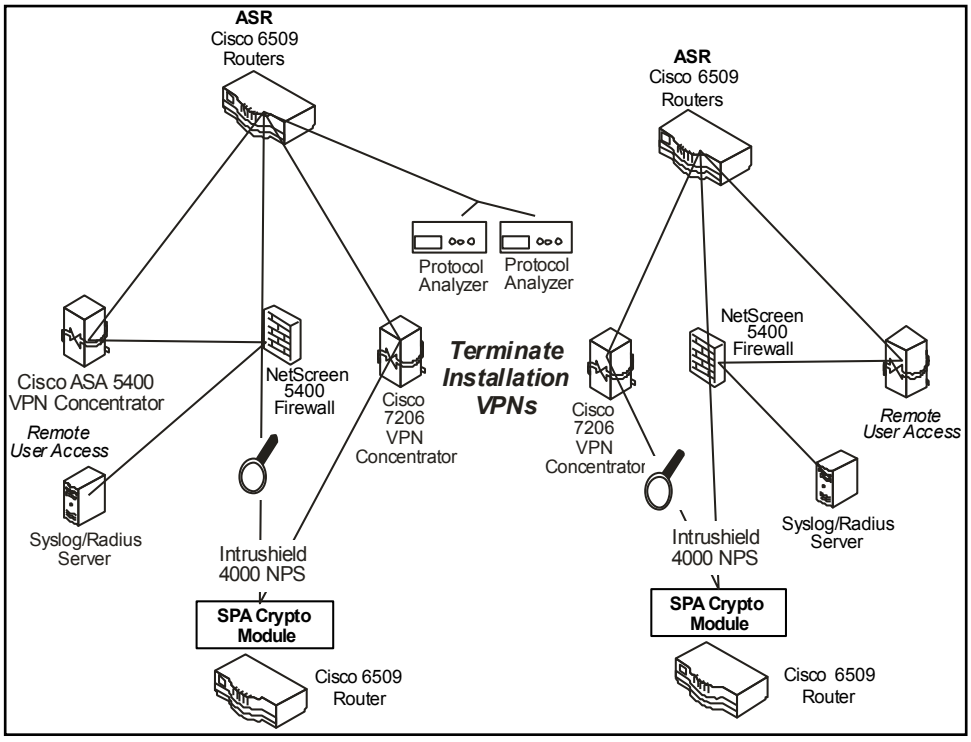

Figure 2-1. Basic network and information systems protection measures

2-51. Protection against intrusions into friendly computer networks by denying unauthorized entry and access into these systems is essential for network and system protection. OPSEC procedures allow the commander to identify actions that adversary intelligence systems and intruders observe. It provides an awareness of the indicators that adversary intelligence systems might obtain. OPSEC identifies and selects information that is subject to exploitation by adversaries and identifies countermeasures that reduces risk to an acceptable level. Since most intrusions result from human error, training in OPSEC is one measure that protects against intentional and unintentional intrusions. Many different measures affect OPSEC, including information security, transmission security, COMSEC, and signal security.

2-52. New global commercial capabilities (including imaging, positioning, and cellular systems) offer potential adversaries access to an unprecedented level of information about our forces. Army and other service personnel can send information directly from the battlefield via e-mail to points around the world from most areas of operation. These e-mails may contain sensitive or classified information, and if disclosed, could endanger US personnel and compromise missions.

2-53. Information provided on Army Web pages is also a security concern. For Web pages, the OPSEC guidelines are the same as any other information available within the Army. Sensitive and classified information needs protection against disclosure to unauthorized personnel. Refer to https://www.acert.1stiocmd.army.mil for specific guidelines on Web site administration policies, procedures, and network security tools.

2-54. As more of the Army's information flow transitions to network enabled communications, information security takes on an ever-growing importance for protecting information management. Units rely on computer systems and networks for logistics, personnel, administration, maintenance, and financial data processing and transfer in both war and peace. These critical networks and systems are vulnerable to intrusions and attack at every echelon in the Army. The Internet is the preferred communications platform for intruders to launch an attack or intrusion. Normally, the intruder's IP address is difficult to track, making it impossible to apprehend the perpetrator.

2-55. Security measures and procedures must actively and passively preserve the confidentiality, integrity, and functionality of information systems throughout the LWN. Protection includes real and near-real-time measures that detect intrusions and then restore the affected device or system. Security measures that assist in protection include—

- Adopting vigorous IA protection programs.
- Denying unauthorized access.
- Hardening programs and gateways with specific software and hardware means.
- Developing procedures for quality assurance in all program and hardware acquisition.
- Strict access control for use of networked computers and other devices.

2-56. US forces must be assured that the expanded communications system infrastructure can attain the level of protection required for mission success. Service providers, the DOD, and other government agencies must cooperate to implement this or any other level of protection for the GIG.

2-57. The technical complexity of information infrastructures may inhibit a commander's ability to manage the information available. Additionally, the availability of information dissemination devices (such as e-mail) may prove to be a menace to the security of information that originates from the battlefield. Currently, the DOD has taken steps to restrict the entrance into sensitive information areas, critical network nodes, and the elements of the GIG. Several initiatives are underway to protect the US information infrastructure from intrusions and attacks.

2-58. Close coordination with the supporting judge advocate is critical in confronting information security challenges at each network management level. Network managers must be aware of regulations, statutes, and public laws that govern privacy and monitor activities. Due to recent disclosures of sensitive or classified information using networked computers, legislation may change regulations and laws that govern monitoring activities of the various government agencies. If approved, these changes will allow law enforcement agencies greater access and authorization to search computers and files used by government

workers (military, civilian, or contractors) when suspected of unauthorized transfer of information. Only authorized investigation agencies (e.g., the Federal Bureau of Investigation and Criminal Investigation Division) will perform these investigations. Under present federal and state laws and statutes, most counter-attack actions are illegal.

2-59. Transmission security secures information across the various networks. Trunk encryption devices, in-line encryption devices, COMSEC, frequency hopping, and time division techniques usually secure transmissions. Transmission security ensures information security when using one or more of these techniques or devices. All systems must operate in SECRET systems high mode to prevent the intrusion into information systems. Any non-secure system or device connected to, or entering, any secure network must have an inline encryption device in use between the network entry point and the entering equipment. This ensures complete network security. In some cases there may be a requirement to send information across domains. In these cases a cross domain solution is required. A cross domain solution is "An information assurance solution that provides the ability to manually and/or automatically access and/or transfer information between two or more differing security domains." (Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 6211.02B) A security domain is a system or network operating at a particular sensitivity level.

2-60. COMSEC in networks and system devices is essential in order to protect the networks information. Specific keys enable secure encryption of the voice and data passed through transmission devices and computers. The National Security Agency controls most encryption keys and governs local key generation, distribution, and storage of these materials.

2-61. Information security policies deny unauthorized persons access to classified or sensitive information during electrical transmission from the sender to the receiver. They establish requirements designed to prevent the disclosure of valuable information from other aspects of communications (for example, traffic flow and message analysis) and to enhance the authentication of communications. (See AR 380-5, AR 380-40, and Technical Bulletin 380-41 for additional information on COMSEC.)

2-62. Demonstrations in the banking industry have shown how vulnerable encoded systems are to any individual or adversary with the help of ordinary computer technology. The demonstration validated that the civilian sector and government agencies are subject to intrusions and attacks from ordinary sources using current, state-of-the-art technology. Though the demonstration focused on encryption keys of less complexity than used in the Army, it reiterated that good COMSEC procedures and password control must be followed at all times.

2-63. The information operations condition (INFOCON) system provides a framework for commanders to increase the measurable readiness of the networks to match operational priorities. The Army maintains the general status of its networks and information systems by using INFOCON reporting procedures. The INFOCON provides a coordinated, structured approach of defense against, and reaction to, attacks on DOD computers, networks, and information systems. IT, increased system connectivity, and standoff capability make computer network attacks attractive to adversaries of the US. INFOCON outlines countermeasures to scanning, probing, unauthorized access, and data browsing. See the Army Global Network Operations and Security Center (A-GNOSC) and Army Computer Emergency Response Team Tactical Operations Center (A2TOC) Web page https://www.acert.1stiocmd.army.mil for the INFOCON status. The INFOCON statuses are—

- INFOCON 5—NETOPS procedures IAW Strategic Command Directive 527-1.
- INFOCON 4—increased military vigilance procedures.
- INFOCON 3—enhanced readiness procedures.
- INFOCON 2—greater readiness procedures.
- INFOCON 1—maximum readiness procedures.

DETECTION

2-64. Real-time security management and intrusion detection should be included in routine operations for NOSCs. To detect occurrences that constitute violations of security policies, selected events or occurrences

(such as numerous log on attempts within a specified period) are monitored using conventional protection and detection tools and devices. When violations are detected, the network manager must prevent further violations and report the event to the commander, information assurance security officer (IASO), TNOSC, and regional computer emergency response team (RCERT).

2-65. NOSCs (such as the A-GNOSC and TNOSC) provide near real-time surveillance for networks and systems to detect suspicious security events and initiate preliminary defensive actions to block or contain the attack in order to minimize the operational impact. Robust and resilient infrastructure architecture isolates and controls the damage from attacks, and makes these systems readily repairable in case of attack. The fundamental criteria are that no single attack leads to failure of a critical function, and no single protection mechanism protects critical functions or systems.

2-66. Network managers and users must train in all aspects of information systems security on the systems they operate and maintain. They must maintain the audit functions and review audit information for detection of possible system abuse. They must also coordinate with the information assurance manager (IAM), information assurance network manager (IANM), IASO, and other appropriate agencies when violations occur.

2-67. Appropriate safeguards detect and minimize unauthorized access and inadvertent, malicious, or non-malicious modification or destruction of data. Appropriate detection safeguards ensure security classification labels remain with data transmitted via a network to another information system.

2-68. Security management devices and IAVMs warn NOSC personnel of intrusion attempts, attacks, and other anomalies for networks and systems. The response to these alerts depends on the severity of the attack, intrusion, or breach. Appropriate reactive measures must be taken when problems occur. Network managers need to consider operational status or mission status before responding to alerts. The information systems protection concept envisions real-time security management as a component of NETOPS as well as being incorporated into the operations. When detection occurs, network managers may need to take the following actions—

- Change boundaries and perimeters.
- Reconfigure firewalls, guards, and routers.
- Reroute traffic.
- Change encryption levels or re-keys.
- Zeroize suspected compromised communications.
- Re-establish a net without selected members.
- Change passwords and authentication.

PASSWORD CONTROL AND AUTHENTICATION

2-69. Since 31 JUL 06, access to all Army networks is mandated to be via the Common Access Card only. This was mandated by the Army Password Standards Version 2.5. Passwords are an important aspect of computer security and are used to achieve authenticated access control at the workstation or host level for authenticating user's access to Army resources until Common Access Card is implemented or for personal use. A poorly chosen password may result in the undetected compromise of an Army network or unlawful usage of Army systems. As such, all users, employees, including contractors and vendors, with access to Army information systems, are responsible for taking the appropriate steps to select and secure their credentials. The commander's designated representative oversees generation, issuance, and control of all passwords. Password issuance is performed IAW AR 25-2. Basic password guidelines are—

- After generation, password handling and storage are at levels of the most sensitive data contained in the system. Password issuance is only available to users authorized to access the system.
- At the time of password issuance, all users will be briefed on—
    - Exclusiveness, classification, and uniqueness of each password.
    - Safeguard measures required for classified and unclassified passwords.

- Prohibitions against disclosure to anyone, to include personnel assigned to the same project and holding identical clearances.
- Immediately informing the IASO of password disclosure, misuse, or other potentially dangerous practices.
- One time issuance of password.
- Retirement of passwords when the time limit has expired or the user has transferred to other duties, been reassigned, retired, or been discharged or otherwise separated from the duties or the function for which the password was required.
- Passwords, as unique identifiers of individual authority and privileges, are strictly for use by one user.
- Changing all passwords IAW AR 25-2.
- Protection of passwords against unauthorized observation on terminals and video displays.

- In addition to a password, a user can be authenticated by something the user possesses (token), or a physical characteristic (biometric).

REACTION

2-70. Reaction to a network or information system intrusion incorporates the capability to restore essential information services and initiate IO attack response processes. Establishing a disaster recovery capability requires devising restoration procedures in a detailed COOP plan. The plan should address various levels of restoration depending on the number of possible disasters. Immediate restoration capabilities may rely on backup or redundant network links or system components, backup databases, or even alternative means of information transfer services.

2-71. Network managers do not require permission to react to attacks or intrusions if their activities are IAW appropriate regulations, statutes, and public law. Upon verification that an intrusion has occurred, network managers or the system administrators must take the following emergency steps:

- Stop the breach, if possible, and restore any destroyed or compromised data from backups and other identified COOP capabilities.
- Follow network security incident policy, as outlined in the standing operating procedure and other applicable regulations.
- Report the incident to the commander, IAM, or IASO and the supporting RCERT immediately.
- Report the incident to other control facilities, as required.

2-72. The response processes begin when the emergency is under control and information services are restored. Responses can be offensive or defensive. Offensive measures are restricted to law enforcement agencies during peacetime operations. During hostilities, the commander may use military force to eliminate or disrupt the means or systems an adversary uses to conduct an information attack. Defensive responses include all measures and countermeasures available to a commander to limit an adversary's attack, exploitation, or deception, or an electronic warfare capability to protect against further attacks.

Note. A network manager, systems administrator, or user performs only defensive actions. They do not perform offensive actions, such as hacking into adversaries' computers or launching computer attacks.

ROLES AND RESPONSIBILITIES

2-73. All network and information system users are responsible for the security of the terminal devices and transmission media they use. AR 25-2 describes the information systems security program and the authority for protecting these systems. It requires structured physical and network security programs that include

security personnel and procedures to combat intrusions into networks and information systems. Specific organizations and personnel within DOD protect against, detect, and react to intrusion and attacks to the US information infrastructure. The following paragraphs discuss the roles and responsibilities of the organizations and personnel that play an integral part in IA at the numbered Army, corps, division, and BCT.

2-74. The *Unified Command Plan 2004*, dated March 2005, assigns CDRUSSTRATCOM as the CCDR for IO and global communications system intelligence, surveillance, and reconnaissance. CDRUSSTRATCOM has determined that this mission includes directing global network operations (GNO), advocating the NETOPS requirements for all combatant command (command authority) (COCOM), and planning and developing national requirements.

2-75. JTF-GNO directs the operation and defense of the GIG to assure timely and secure network enabled capabilities across strategic, operational, and tactical boundaries in support of DOD's full spectrum of warfighting, intelligence, and business domains.

2-76. The commander, JTF-GNO, will exercise operation control (OPCON) of the GIG for GNO issues. Under the authority of CDRUSSTRATCOM, JTF-GNO issues the orders and directives necessary to maintain the assured service of the GIG, ensuring that the President, Secretary of Defense (SECDEF), combatant commands, services, and agencies (CC/S/A) can accomplish their missions. The CC/S/A executes the JTF-GNO's directives within their respective areas and report compliance.

DEFENSE INFORMATION SYSTEMS AGENCY

2-77. DISA performs significant NETOPS support functions. DISA manages OPCON over information services, IT environments, and computing processing centers for all DOD components. For additional information regarding the roles and responsibilities of DISA, refer to Chapter 3.

2-78. DISA also provides the Department of Defense-Computer Emergency Response Team (DOD-CERT), which is the information security incident response support to the GIG community for IA. The DOD-CERT identifies, analyzes, assesses, and resolves all information security vulnerabilities and exploitations in the GIG to support the DISA's IA mission. The DOD-CERT works closely with service response teams and organizations to combat the threat of attacks and intrusions into the GIG.

DEPARTMENT OF DEFENSE-COMPUTER EMERGENCY RESPONSE TEAM

2-79. The DOD-CERT is under OPCON of the JTF-GNO and serves as the primary network or information system intrusion response capability within the DOD. It helps identify, assess, contain, and counters attacks that threaten IO across the spectrum of military operations. In addition to the DOD-CERT, the services establish computer emergency response teams (CERTs) to provide an effective CND for their portion of the GIG. The Army infrastructure consists of an A2TOC, RCERTs, and local CERTs. They work with other security agencies to minimize or eliminate identified vulnerabilities to networks and information systems. Their major capabilities include—

- Identifying and resolving computer security anomalies that affect the GIG's ability to support the Soldier.
- Identifying threats to networks and information systems; developing, disseminating, and implementing countermeasures to these threats.
- Assessing the incidents reported and determining the impact on the Soldier's ability to carry out his mission.
- Coordinating the response actions taken by the organizations experiencing intrusions.
- Serving as the technical advisor on all protection measures.

JOINT TASK FORCE-GLOBAL NETWORK OPERATIONS

2-80. The commander, joint task force-global network operations (CJTF-GNO) will exercise OPCON of the GIG for GNO issues. To achieve this mission, CDRUSSTRATCOM assigned these tasks to the CJTF-GNO:

- Maintain direct operations and defense of the GIG.
- Maintain GIG availability and integrity; ensure efficient traffic management.
- Establish and oversee SA of the GIG readiness and defensive posture.
- Assist CDRUSSTRATCOM in developing tools, monitoring threats, verifying policy compliance, and controlling network access for consistent IAVM.
- Direct and oversee network defense and information services.
- Assist in establishing and maintaining standards for network, component, and defensive requirements.
- Conduct network defense planning, preparation, and operations employment for normal operations and for crisis and deliberate planning. When directed, support deliberate and crisis action planning requested by other CCDRs.
- Develop, coordinate, integrate, direct, and oversee specific network defense courses of action in support of GIG NETOPS and defense. Coordinate with CDRUSSTRATCOM for approval authority on Tier 2.1 CND response actions.
- Support United States Strategic Command (USSTRATCOM) participation in exercises and experiments involving GIG network management and defense.
- Provide intelligence requirements in support of network defense.
- Provide assessments and recommendations to USSTRATCOM for watch condition (WATCHCON) changes dictated in network threat warning.
- Provide recommendations to USSTRATCOM for INFOCON changes.
- Direct and oversee the establishment and maintenance of standards for technical testing, evaluation, and measures of effectiveness of NETOPS and defense capabilities.
- Direct and oversee establishing procedures to provide department measures of effectiveness and battle damage assessment during and following network defense operations.
- Assist in formulating guidance for training NETOPS and defense forces.
- Assist in developing and promulgating joint tactics, techniques, and procedures for NETOPS and defense activities.
- Identify desired characteristics and capabilities for NETOPS and defense.

2-81. USSTRATCOM has assigned the GNO mission to the JTF-GNO, which was formed by the merger of the DISA Global Network Operations and Security Center (GNOSC) and JTF-GNO. The JTF-GNO is staffed 24 hours a day, seven days a week. Due to the merger, the JTF-GNO can take advantage of the existing intrusion detection capabilities of the unified commands, its components, and DOD and non-DOD agencies. The joint task force (JTF) receives intrusion data from these sources and then fuses this critical information with ongoing operational missions and intelligence and technical data into a synopsis of the incident.

2-82. United States Army Space and Missile Defense Command (USASMDC)/United States Army Forces Strategic Command (ARSTRAT) is the Army Service component command (ASCC) to USSTRATCOM and directly supports the JTF-GNO. USASMDC/ARSTRAT is also USSTRATCOM's primary point of contact for all Army NETOPS and CND missions. USASMDC/ARSTRAT plans, integrates, and sustains Army CND and is the communications system advocate. The commander, USASMDC/ARSTRAT has designated the Commanding General (CG), NETCOM/9th SC(A) as the USASMDC/ARSTRAT deputy for NETOPS to represent USASMDC/ARSTRAT in communicating and coordinating directly with DOD and USSTRATCOM regarding NETOPS. (Refer to Figure 2-2.)

CHIEF INFORMATION OFFICER G-6

2-83. The CIO G-6 establishes policy and procedures to manage a cohesive AIAP. The CIO G-6 is the focal point for managing and implementing the AIAP. The CIO G-6 reviews and evaluates proposed policies, procedures, directives, doctrinal publications, plans, materiel requirement documents, life-cycle management documents, basis of issue plans (BOIPs), and similar documents with IA implications. Additional responsibilities include—

- Evaluating technological trends in IA and establishing a methodology to integrate advancements into networks and information systems.
- Providing IA policy to Army elements to include assisting PEOs and program managers in identifying and incorporating IA requirements in the development of new information systems.
- Acting as the Army proponent for the IA training and awareness program.
- Providing direction, procedures, and guidance on IA protection measures to all Army support organizations.
- Developing certification requirements for system administrators, network managers, and IA personnel (information assurance program manager [IAPM], IANM, IAM, and IASO).

Note. AR 25-6 uses IAPM, IANM, IAM, and IASO as replacements for the information systems security program manager, information systems security manager, and information systems security officer used in AR 25-2.

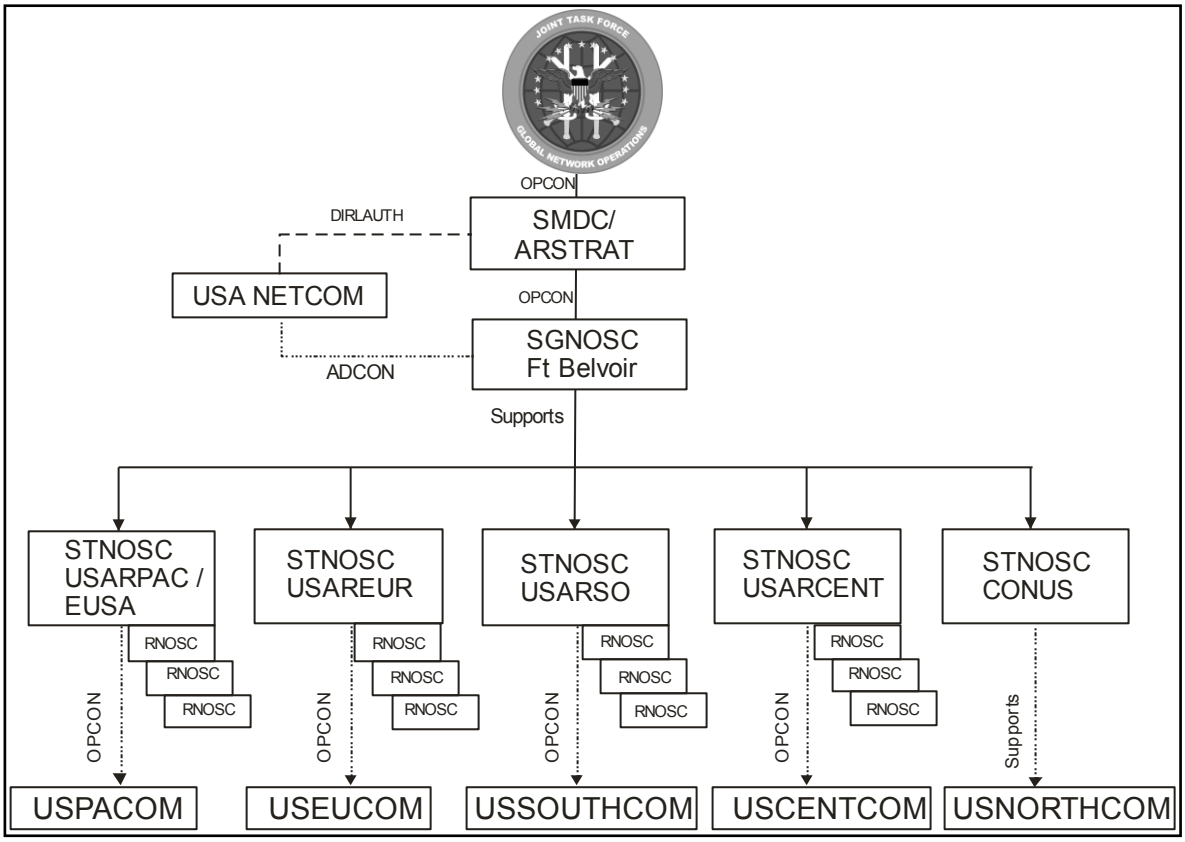

Figure 2-2. US Army Space and Missile Defense Command/US Army Forces Strategic Command

NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND (ARMY)

2-84. The NETCOM/9th SC(A) is responsible for the operations, management and defense of the LWN to include centralized intrusion detection and monitoring worldwide. Collocating and integrating the operations of TNOSCs with the 1st Information Operations Commands (IO CMDs) RCERTs providing a common view of all detected network and host intrusion events to the strategic and tactical units worldwide.

2-85. This collocation provides theater and below support by monitoring, detecting, and responding to incidents within their AOR. The RCERTs provide training within their AOR and conduct local coordination with Army criminal and counterintelligence assets. They also disseminate information and reports throughout their AOR and to the A2TOC for further analysis and dissemination.

2-86. NETCOM integrates and coordinates the execution of NETOPS to include CND support to USSTRATCOM/JTF-GNO. Through the A-GNOSC, NETCOM/9th SC(A) is responsible for global NETOPS and CND actions across the entire Army LWN. The A2TOC, maintains/provides daily NETOPS and CND SA to Army and Joint leadership. The A2TOC will provide recurring reports (e.g. commander's critical information requirement, operational, situational) and, if applicable, day-to-day actions and preplanned NETOPS and CND operations directly to JTF-GNO and USASMDC/ARSTRAT.

ARMY GLOBAL NETWORK OPERATIONS AND SECURITY CENTER AND ARMY COMPUTER EMERGENCY RESPONSE TEAM TACTICAL OPERATIONS CENTER

2-87. The A-GNOSC and Army computer response team (ACERT) operate the A2TOC. The A2TOC is the single focal point for Army NETOPS. As part of NETOPS, 1st IO CMD and the 2nd Battalion, 1st IO CMD are in direct support of the Army for all CND and CND response action.

2-88. All IA security incidents and vulnerabilities for the Army are reported to the A2TOC as the Army's single focal point. The A-GNOSC is responsible for IAVM. All IAVM messages are posted to Army Knowledge Online (AKO) NIPRNET and SECRET Internet Protocol Router Network (SIPRNET), and all IA personnel are required to subscribe to the AKO Knowledge Management Center to receive IAVM notifications. The IAVM message are used to notify directorates of information management (DOIMs), regional chief information officer (RCIOs), IAPMs, network managers, IAMs, IASOs, system administrators, and eventually users of incidents, vulnerabilities, and other potential network security events.

2-89. The A2TOC monitors, detects, and prevents network and information system attacks. It also conducts vulnerability assessments and responds to Army IA security incidents. The A2TOC leverages and integrates intelligence support from counterintelligence, OPSEC staff, and law enforcement agencies. ICW the A2TOC, theater teams and other Army NOSCs unify the CND effort across Army networks.

INFORMATION OPERATIONS TRIAD

2-90. The CIO G-6, the Deputy Chief of Staff for Operations and Plans, and the Deputy Chief of Staff for Intelligence form the Information Assurance Triad. In a coordinated effort, these agencies implement procedural and material protective measures, develop plans and policies, and validate requirements to protect command, control, communications, computers, and intelligence systems. The CIO G-6 has overall responsibility and oversight for the ACERT program.

2-91. The Deputy Chief of Staff for Operations and Plans IA responsibilities, as they relate to the ACERT program, consist of providing staff support and OPCON of the 1st IO CMD.

2-92. The Deputy Chief of Staff for Intelligence IA responsibilities, as they relate to the ACERT program, include—

- Identifying the threat and establishing policy for integrating intelligence support.
- Identifying computer network attack capabilities targeted against friendly information systems.
- Promulgating the information systems security monitoring policy.

Note. See AR 25-2 and pertinent security and intelligence regulations for additional AOR specific details of these agencies.

1ST INFORMATION OPERATIONS COMMAND

2-93. 1st IO CMD, through the ACERT and in conjunction with the A-GNOSC, provides CND for the LWN. The ACERT analyzes operational information relating to threats to the LWN; supports the Army with attack sensing and warning, indications and warnings; and synchronizes and executes global CND operations in support of Army and joint forces worldwide.

NOSC AND CERT RELATIONSHIP

2-94. The NOSCs and CERTs assist in the war against attackers, intrusions, viruses, and other technical complications when needed. They are collocated, enabling the organizations to work closely together to protect network and information systems.

2-95. The ACERT and RCERT use specific security and vulnerability assessment tools (e.g., scanning tools) for network and systems evaluation. These CERTs will enter equipment, networks, and systems only at the request of the commanders or the equivalent responsible person. (Refer to AR 25-2 and AR 380-53 for specific authorizations and details of these missions.)

2-96. The A-GNOSC, TNOSCs, and other NOSCs perform their GND duties IAW AR 25-2. The NOSCs and CERTs may also perform duties IAW other pertinent SOPs, regulations, and public laws.

2-97. Reporting procedures for incidents of intrusions and attacks flow vertically and horizontally to all levels of the chain of command, system administrator, IASO, IAM, DOIM, RCIO, theater team, A2TOC, and JTF-GNO. This flow of information allows for notification and an area view, by authorized organizations, to combat an all-out attack against networks, systems, computers, and the GIG.

2-98. The commander, network manager, or user notifies the local IASO and IAM when he detects an actual or potential security incident or intrusion. The IASO or IAM then reports the incident or intrusion to the supporting CERT and NOSC. The CERT works with the network manager and customer to identify the problem, remove the threat, and recover from the incident. These teams respond to incident reports and coordinate actions IAW CJCSI 6510.01E, Chapter 1, appropriate service regulations, and public laws.

INFORMATION ASSURANCE PROGRAM MANAGERS

2-99. An IAPM is appointed at each Army command (ACOM) and PEO. The IAPM establishes, manages, and assesses the effectiveness of the IA program at that command or activity. The IAPM manages the personnel who perform the computer security and COMSEC sub-disciplines of IA. AR 25-2 contains a complete list of responsibilities for all IA personnel. Other responsibilities of the IAPM include—

- Establishing and managing a command IA program and developing an IA policy based on command-unique guidance.
- Establishing and overseeing an IA training and accreditation program that integrates IA into operational training programs for managers, system administrators, and users.
- Coordinating and reviewing operational concepts, SOPs, and security accreditation for command and control systems.
- Chairing the ACOM IO Triad, ensuring IA standards and programs are enforced.
- Ensuring an ACOM IANM is appointed.
- Ensuring IAMs are appointed at designated echelons below the ACOM.
- Serving as the ACOM point of contact for IAVM advisories and managing the command IA incident reporting program.

ARMY COMMAND INFORMATION ASSURANCE NETWORK MANAGER

2-100. An ACOM IANM is appointed to support the IAPM with network security and the command IA program. Specific responsibilities include—

- Developing and staffing IA technical policy and procedures for all ACOM-unique networks and information systems.
- Ensuring that all networks and information systems are planned, installed, managed, maintained, and properly accredited IAW AR 25-2.
- Ensuring that all IA command policies are implemented.
- Assisting the IAPM in monitoring and enforcing the IAVM process.

INFORMATION ASSURANCE MANAGER

2-101. An IAM is appointed at the appropriate levels of command below ACOMs, which include major subordinate command, post, camp, and stations. Where there are multiple IAMs, the installation IAM will be designated as the senior IAM. The responsibilities of the IAM include—

- Developing, staffing, and managing IA plans for his AOR.
- Conducting individual network and information systems risk assessment to determine potential threats and vulnerabilities, and determining appropriate measures to effectively manage the risks.
- Conducting IA training and awareness programs.
- Implementing IA and IAVM reporting and compliance procedures, to include IA incidents and technical vulnerabilities.
- Ensuring that an IASO is appointed for each network and information system, and an IANM for each installation or NOSC.
- Establishing the scope of responsibility for each IASO.

INFORMATION ASSURANCE NETWORK MANAGER

2-102. The IAM appoints an IANM for each installation or group of networks to provide direct support to the IAM. The responsibilities of the IANM include—

- Implementing the IA program for networks IAW policy received from the appropriate network security manager, the IAPM, and the IAM.
- Ensuring procedures are in place to support security integrity of the network, providing protection for the network, and supporting secure access controls and connectivity.
- Developing and implementing security procedures and protocols.
- Conducting reviews of network threats and vulnerabilities, and reporting any attempts to gain unauthorized access to the network.
- Implementing IA and IAVM reporting and compliance procedures to include the use of only Army-approved IA products.

S-2 AND G-2

2-103. The intelligence staff officer (S-2) and assistant chief of staff, intelligence (G-2) identify and assess foreign intelligence threats directed toward command assets and functions. Within the context of NETOPS, this staff officer will consider the threats to the command's information systems and networks as part of his overall intelligence support program by—

- Being engaged in the reporting of IA-related security violations and incidents to the servicing RCERT IAW Section VIII, Incident and Intrusion Reporting of AR 25-2.
- Including IO and IA requirements in submissions of commander's critical information requirements or priority intelligence requirements.
- Providing technical and non-technical information to support a commander's INFOCON program.

- Providing a means for commanders, risk managers, IAMs, and IANMs to request intelligence to fill knowledge gaps about threats to information systems and networks during any phase of the IA program process.

G-6

2-104. The G-6 has overall responsibility for the secure operation of network and information systems at all levels. The G-6 assumes the responsibilities of the IAM, supervises the IANM, and oversees the actions of the IASOs in the subordinate units.

INFORMATION ASSURANCE SECURITY OFFICER

2-105. The IASO is an additional duty appointed by the commander for each information system or group of systems. The IASO—

- Prepares, distributes, and maintains plans, instructions, guidance, and SOPs for command and control systems security.
- Prepares or oversees the certification and accreditation documentation of systems IAW AR 25-2.
- Coordinates with the brigade S-2 to ensure users have the required security investigations, clearances, authorizations, and need-to-know.
- Establishes and implements a system for issuing, protecting, and changing systems passwords.
- Establishes the training and awareness programs.
- Monitors and ensures the proper security of systems connected to the network.
- Assesses direct threat and vulnerability, enabling the commander to analyze the risks to interconnected systems.
- Determines appropriate measures to manage network risks effectively.
- Oversees the review of network and information systems audit trails, resolves discrepancies, and reports incidents to the brigade or battalion S-2 for evaluation and reporting.
- Performs assigned password control duties.

S-6

2-106. The command, control, communications, and computer operations (S-6) have overall responsibility for the secure operation of the network and information systems at BCT and subordinate units. At the BCT, the S-6 normally assumes the role and responsibilities of the IASO unless otherwise appointed by the commander. The responsibilities of the S-6 include—

- Advising the commander on recommended IA policy updates.
- Determining the network plan for IA to distribute the IA tools to the network and information system managers.
- Downloading the appropriate tools as they are updated or as new tools are introduced.
- Downloading and distributing the current network IDS, attack and virus files, and the relevant software security patches.
- Monitoring the network IDS and network IPS for possible attacks and reconfiguring the network, if necessary.
- Ensuring that password integrity is maintained.

S-3

2-107. The operations staff officer (S-3), as the operations officer for signal units at the numbered Army, corps, division, BCT, and battalion, supervises the IANM and the operation of the Information Analysis Center. The Information Analysis Center resides within the NOSC and consists of several workstations that monitor a variety of IA software applications and tools.

USER

2-108. Each information systems user is responsible for security. The user—

- Secures operations of his information systems.
- Operates his terminal IAW equipment operation procedures and SOPs.
- Performs other duties as assigned by the IASO and network manager to ensure security and protection of network and information systems.
- Follows regulatory and policy restrictions for authorized use of government equipment.
- Reviews and complies with user responsibilities outlined in AR 25-2.
- Reviews and acknowledges the Acceptable Use Policies as provided by the IASO.

INFORMATION ASSURANCE TOOLS

2-109. A variety of software and hardware tools enable network managers and IANMs to prevent, detect, monitor, and evaluate intrusions into their networks. These tools change continuously as technology evolves, and they must be CIO G-6 approved. The CIO G-6 approves the current list of protection tools and distributes them to subordinate activities, as necessary. The A2TOC and RCERTs maintain these tools and software on their Web sites for downloading by network managers and system administrators. (Refer to Appendix B for a detailed discussion of the different systems and tools available to perform the required NETOPS functions). Protection and detection tools include—

- Audit monitoring and IDSs and IPSs.
- Isolate systems under attack by automated infrastructure management.
- Detect malicious codes and eradicate systems.
- Analyze and assess vulnerability.

2-110. To protect against external and internal attackers and virus attacks the RCERT and A2TOC recommend, and the IANM enforces, the following hardware and software tools:

- Antivirus software.
- Hard-disk purge capability.
- Network mapping software.
- Audit profile software.
- IDSs and IPSs.
- Secure password generation systems.
- Inline network encryption devices.
- Firewalls, high-assurance guards, and tactical security guards.
- Encryption key management systems.
- Security posture of networks and systems.
- Host Base Security System.
- Patch Management System.
- Vulnerability Scanning Systems.

INCIDENT AND VULNERABILITY REPORTING

2-111. Any user noticing abnormal or suspicious activity must report it to his chain of command, IAM, IANM, IASO, and CERT. The internal staff reporting will be designated by local SOP. Refer to the A2TOC Web site at https://www.acert.1stiocmd.army.mil, the DOD-CERT Web site at https://www.cert.mil/, or CJCSI 6510.01E, Chapter 1 for details on incident and vulnerability reporting. Detection of security incidents may cause users or network managers to conduct—

- **Logging**. Recording security-relevant information to facilitate detection and investigation of security breaches IAW applicable regulations, statutes, and public laws. All devices require reporting the event to an audit manager.

- **Local reporting**. Specific security-relevant events and violations will follow reporting procedures to the IAM, IASO, S-3, G-6, and S-6 depending on the incident and reporting process.
- **Remote reporting.** The IAM, IASO, S-3, G-6, and S-6 evaluate security-relevant events and report the specific occurrences through the chain of command and operational structure to the CERTs.
- **Recovery actions**. After a security breach, implementation of recovery actions occurs throughout the affected networks and equipment.

INFORMATION ASSURANCE VULNERABILITY MANAGEMENT

2-112. The IAVM message is another method used throughout to report vulnerabilities. The A-GNOSC is the Army's focal point for the implementation of the IAVM process. The AKO Knowledge Management Center mail service, on behalf of the A-GNOSC, issues alerts, bulletins, technical tips, and system administrator reports. These messages are based on both mandatory JTF-GNO information assurance vulnerability alert (IAVA) messages and Army generated IAVM requirements. The A-GNOSC messages direct specific actions (protect, detect, and react) and establishes mandatory suspense dates for compliance. See the A-GNOSC Web site at https://www.us.army.mil/suite/portal.do?$p=138011 for more information concerning IAVM policies.

2-113. IAVM is the DOD program to identify and resolve discovered vulnerabilities in Army systems and platforms. It requires the completion of four distinct phases to ensure compliance. These phases are: (1) vulnerability identification, dissemination, and acknowledgement; (2) application of measures to affected systems to make them compliant; (3) compliance reporting; and (4) compliance verification. This program includes IAVAs, information assurance vulnerability bulletins (IAVBs), and technical advisories.

2-114. A patch is an immediate solution provided to users once a bug is discovered and can often be downloaded from the software maker's Web site. Previously, patches required a manual touch at each device on the network coupled with the length of time an automated tool was required. An enterprise solution has been selected by the DOD which is Eye Retina for scanning and Citadel Hercules for remediation.

2-115. Complete asset inventories (100 percent) will be conducted and reported to the Army Asset and Vulnerability Tracking Resource (A&VTR) Database semi-annually as a minimum and after every IAVM. Training is to be recorded in the Army Training Command database at https://atc.us.army.mil/iastar/index.php. Dissemination of IA technical advisories, IAVBs, and IAVAs will automatically be forwarded upon registration completion. Interoperability testing will be performed prior to the application of system patches and fixes for interoperability compliance.

2-116. All IAVMs will be applied immediately. If the IAVM cannot be implemented, a mitigation plan must be submitted in A&VTR for approval/disapproval.

SCANNING AND REMEDIATION

2-117. Scanning is the gathering of information on information systems and device configurations, which may be used for system identification, maintenance, security assessment and investigation, vulnerability compliance, or compromise. This includes network port scanning and vulnerability scanning, whether wired or wireless, classified or unclassified. Scanning is conducted throughout all phases of operation (phases 0-4).

2-118. An operational scanning capability will be retained at the unit level as well as layered throughout the enterprise operational management structure for all classifications of networks. Regular, scheduled, and no-notice scans are integral to Security Policy and Compliance Enforcement and shall be done at all levels and all operational networks. Scanning tools may be obtained through Communications Security Logistics Activity.

2-119. Assessors must use a five step methodology for assessment scanning as follows: identify assets, determine vulnerabilities, review vulnerabilities, remediate vulnerabilities, and validate remediation measures. All new information systems and device vulnerabilities must be proactively managed.

2-120. System administrators/Network managers must identify and prioritize which systems are most critical and develop a protection strategy. System administrator/Network managers and IA personnel will perform routine and scheduled unit vulnerability assessments and management in addition to IAVM procedures to manage system and network vulnerabilities proactively and to maintain the necessary skill sets to remediate vulnerabilities proficiently, whether these networks reside with generating or deployed forces. The system administrator/network manager needs the consent of the IASO and G-6/S-6, who will consider operational or mission status and tactical bandwidth constraints before scanning. Table 2-1 details the actions that must be conducted when scanning.

Table 2-1. Scanning guidelines/actions

Step	*Scanning guidelines/actions*
1	System administrator will obtain and maintain training and certification on Army approved IA scanning tools from Communications Security Logistics Activity located at https://informationassurance.us.army.mil/
2	System administrator will review Army Best Business Practices at https://informationassurance.us.army.mil/
3	System administrator will scan network-attached devices with Army-approved products monthly or after receipt of an IAVA.
4	System administrator will review scan reports and determine devices to be patched. Update locally created database/spreadsheet for future reference on false positives.
5	IASO and system administrator will manually or electronically remediate devices requiring patch.
6	IASO and system administrator will rescan network for patch verification.
7	IASO and system administrator will maintain scan results locally and report scan results to the organization commander and IA personnel, DOIM and servicing NETCOM and information management area component, RCIO, functional CIO, RCERT/TNOSC, or ACERT/A-GNOSC.
8	IASO and system administrator will update A&VTR with compliancy information.

2-121. Remediation is defined as the process of correcting a fault or deficiency, or, in this case, vulnerability. The system administrator/network manager will ensure the confidentiality of information by preventing unauthorized individuals access to computer equipment. The system administrator/network manager/operator will patch system security vulnerabilities on all Army platforms. DOIM and tactical unit administrators are required to validate patches whether on the installation network or placed in storage. These requirements should be stated in unit OPORDs and other directives with command.

2-122. System administrators are responsible for reducing the vulnerability of their system through the application of software patches, both hot fixes and service packs. Table 2-2 details the actions taken during the remediation process.

Table 2-2. Remediation actions

Step	*Remediation actions*
1	Implement unit policy, on a weekly basis, directing users to log off their workstations but leave workstations on for application of patches during non-duty hours. Specific day to be determined by the unit IAM.
2	Receive IAVM identifying required patch.
3	Select required patches from the applicable Web site.
4	Ensure individual responsible for IAVM has administrative rights to the assets to be scanned and patched.
5	Scan assets (servers, routers, switches, and workstations) to identify assets that require patch application.
6	Identify “test” machine, apply patch, and scan the machine to confirm patch application.
7	Apply patch to the remainder of assets.
8	Issue Conformance Report (via patch application software).
9	Rescan to validate patch application.

Disaster Recovery/Continuity of Operations

2-123. A contingency plan or COOP is a plan for emergency response, backup operations, transfer of operations, and post-disaster recovery procedures maintained by an activity as a part of its IA security program. A disaster recovery plan/COOP ensures that organizations are able to continue functioning after some catastrophic event and ensures that procedures are defined and in-place to protect and restore the organization's vital data and resume operations. Contingency plans/disaster recovery procedures will be tested at a minimum annually. (For more detailed information on COOP, refer to AR 500-3 and Department of the Army Pamphlet 25-1-2.) A list of objectives for a disaster recovery/COOP include:

- Define the essential systems of the organization.
- Describe the personnel necessary to maintain systems.
- Define the objectives tasked with recovery.
- Provide guidance for appropriate locations, timing, and actions required to restore operations in an emergency.

Note. Appendix C provides scenarios that serve as examples of how many activities might occur and their relationships between each other.

EMERGENCY PROCEDURES

2-124. Some cases require emergency procedures to protect US networks. Local SOPs generally explain these emergencies. The following procedures are carried out only under extreme emergencies or otherwise directed by the commander:

- Notify activities, as required, to enable a proper response.
- Purge systems.
- Zeroize COMSEC devices.
- Destruct classified systems only when capture is imminent.

SECTION III - INFORMATION DISSEMINATION MANAGEMENT AND CONTENT STAGING

OVERVIEW

2-125. Managing and protecting networks and information systems for the users does not alone ensure that relevant information is being provided to the Soldier to gain and maintain information superiority. The management of access and delivery of relevant, accurate information to the appropriate user in a timely, efficient manner and in the proper format is a major component of NETOPS.

2-126. IDM/CS provides the LWN warfighting intelligence and business domains at all levels (strategic, operational, and tactical) with awareness of relevant, accurate information; automated access to newly discovered or recurring information; and timely, efficient, and assured delivery of information in a usable format. These services permit commanders to adjust information delivery methods and priorities for enhanced SA. They also allow information producers to advertise, publish, and distribute information to the Soldier. IDM/CS is accomplished by enabling LWN users to safeguard, compile, catalog, discover, cache, distribute, retrieve, and share data in a collaborative environment. IDM/CS enhances all aspects of the LWN transport capabilities and improves bandwidth utilization.

2-127. IDM/CS will allow NETOPS centers to optimize the flow and location of information over the GIG by positioning and repositioning data and services to optimum locations on the GIG in relation to the information producers, information consumers, and the mission requirements. Some of the objectives of IDM/CS are:

- Enabling commanders to adjust information delivery methods and priorities for enhanced SA.

- Enabling information producers to advertise, publish, and distribute information to the Soldier.
- Enabling users to define and set information needs to facilitate timely and efficient information delivery and/or search information databases to retrieve desired products as required.
- Improving bandwidth utilization.
- Enhancing all aspects of the GIG transport capabilities.

2-128. IDM provides awareness of relevant, accurate information; automated access to newly discovered or recurring information; and timely, efficient delivery of information based on the commander's priorities. It seeks to achieve the right information, arriving at the right place, at the right time, and in a usable format. IDM uses specific processes, services, and applications to provide this information to Soldiers at the strategic, operational, and tactical military operations.

2-129. IDM is the means for efficiently communicating information products (such as video, voice, and data) to commanders and their staffs, and ensuring that they know its availability. It uses a distribution system to integrate the delivery and notification functions of the information producers, consumers, and managers. IDM will enable the Soldiers to do the following:

- Define the types of information needed and have it delivered.
- Define particular information products needed, and deliver them as requested.
- Access data from a variety of information systems and retrieve relevant, accurate information for situational understanding.

2-130. The core IDM/CS services are envisioned to be enterprise wide services used by the entire DOD to ensure information is available to all authorized users. The core IDM/CS services are—

- Content discovery.
- Content delivery.
- Content storage.

JOINT TASK FORCE-GLOBAL NETWORK OPERATIONS AND NETWORK OPERATIONS COMMUNITY GRID CONTENT MANAGEMENT RESPONSIBILITIES

2-131. GCM enables JTF-GNO and the NETOPS community to provide GIG users with an awareness of relevant, accurate information, and automated access to newly discovered information for timely, efficient delivery in a usable format. Again, this is accomplished in large part through SA and the associated instrumentation of the GIG. Capitalizing on the content management framework found within the Net-Centric Enterprise Services and Net-Centric Data Strategy, JTF-GNO will facilitate the placement, posting, and transport of information required by GIG users.

2-132. NETOPS centers at all levels will be responsible for ensuring the content discovery, storage, and delivery services, as well as mitigation, are operating correctly and that information is "maneuvered" to the optimum location on the GIG.

2-133. The IDM/CS services are used by NETOPS centers to ensure that the GIG is optimally delivering the information required by GIG users IAW information delivery priorities. The IDM/CS services will provide NETOPS centers at all levels with:

- Visibility of the information flowing across the GIG and of those systems used to store, catalog, discover, and transport information.
- Tools to view information flows and access, to determine impact to network capacity, and to ensure that user profiles are being satisfied with a reasonable quality of service.
- The capability to prioritize information requirements, determine the sources responsible for providing that information, and stage information content throughout the GIG in support of a given operation.

- The ability to track and maintain knowledge of the various requests and user profiles for information; coordinate changes in the operating parameters of GIG assets; identify new products; review and validate the user-profile database; and develop joint policies and procedures governing information flow across the GIG.

2-134. IDM will also enable commanders to control, secure, and manage the use of networks and information systems by establishing priorities for gaining access to the information products. Commanders can also deny access to critical information and information products to maintain the integrity and non-repudiation of the data. Additionally, IDM will assure timely delivery of critical information elements across the battlefield.

PROVISIONING OF INFORMATION DISSEMINATION MANAGEMENT/CONTENT STAGING

2-135. The following sections outline the IT organizations and their responsibilities concerning the provision of IDM/CS. The following sections detail what is generally required by the information manager across all echelons and phases of deployment. These responsibilities speak to the individual activities and tasks that ultimately provide IDM/CS services to a user.

DIRECTORATE OF INFORMATION MANAGEMENT

2-136. The DOIM mission is to provide information systems and services support to the tenants and business partners on installations, thus facilitating the provision of IDM/CS services. The goal of the DOIM is to provide a focus of leadership for IT and to coordinate IT activities with the installation business partners and customers. The DOIM will:

- Build, test, and provide software distribution packages to the tactical units within its AOR.
- Plan forest synchronization for the tactical units.
- Perform PKI certification for the tactical units.
- Provide technical support for tactical units' organizational unit managers.
- Carry out performance management (monitoring and analyzing) of the tactical units' systems.
- Provide anti-virus signatures to the tactical units' e-mail servers.
- Provide technical support on e-mail servers for the tactical units.
- Schedule and facilitate video teleconferencing for the tactical units.
- Provide multipoint video teleconferencing capability for the tactical units.
- Provide mission specific sensitive and SECRET video teleconferencing service to the tactical units, as required (e.g., classroom, transportable, command and control, and desktop).
- Build the patch package.
- Conduct necessary patch testing.
- Provide Tier 3 support to the tactical units to ensure proper installation of the patch and to ensure that operational integrity of the system(s) is maintained.
- Push the patch package to the tactical units.
- Notify tactical units when patch is successfully installed.
- Maintain procedures to prepare for recovery of information from disasters and execute preparatory procedures in support of the tactical units.
- Operate, maintain, and manage the local control center in support of the tactical units.
- Provide technical support on problems escalated from the tactical units.

BCT, DIVISION, AND CORPS INFORMATION MANAGEMENT

2-137. The unit information management mission insures that IDM/CS services are provided, assessable, and utilized. The unit information manager will—

- Restore to tactical units' critical data in event of disaster.
- Begin the process X.509 certificates and create FORTEZZA cards for tactical units.
- Perform capacity measurement and performance analysis on tactical units' e-mail servers.
- Pull anti-virus signatures to the tactical units' e-mail servers.
- Perform forest synchronization for the tactical units.
- Perform storage services (backup, recovery, archiving) on e-mail servers for the tactical units.
- Apply system and desktop management services (monitoring, account management, CM, and remote control) to the AD systems.
- Apply patch management service to the AD systems.
- Perform capacity and availability monitoring (collect, process, analyze, store, and report) of AD systems.
- Operate and maintain domain name service (DNS) servers.
- Maintain Defense Message System servers, software, and other hardware within the AOR.
- Escalate Defense Message System problems to DISA, if necessary.
- Provide the capability to compose, format, transmit, and receive formal organizational e-mail messages at individual workstations.
- Provide unclassified, sensitive and classified organizational messaging capabilities.
- Perform backup and recovery of the tactical units' AD systems.
- Obtain software distribution packages from the DOIM, regional service center, and regional network operations and security center (RNOSC).
- Maintain a separate and distinct AD forest.
- Receive video teleconferencing services from DOIM, regional service center, and RNOSC.
- Perform systems and desktop management organizational activities.
- Provide technical support to the tactical units on all service management issues.
- Pull, test, and provide software distribution packages to the tactical units.
- Push software distribution packages to the subordinate units.
- Provide additional event management capabilities, such as analysis and correlation of event data, to the subordinate units, as required.
- Operate and configure e-mail servers and clients.
- Perform accounts management.
- Perform resource availability measurements on e-mail servers.
- Monitor e-mail components.

END-USER

2-138. An end-user is an individual who uses the GIG. Within this process, the end-user is the final recipient of all services and processes discussed in this manual. End-users have the following general responsibilities for IDM/CS:

- Access and use authorized IT systems IAW Army policy.
- Forward requests for configuration changes.
- Maintain their desktop at approved configuration.

INFORMATION DISSEMINATION MANAGEMENT PRINCIPLES

2-139. IDM principles support the tenet that disseminating information is one of the primary activities involved in information management. IDM is the communication of relevant information of any kind from one person or place to another, in a usable form, by any means to improve understanding or to initiate or govern action. Information dissemination takes the following two basic forms: broadcast or point-to-point

dissemination. IDM activities should exhibit a judicious combination of broadcast and point-to-point forms of dissemination.

BROADCAST DISSEMINATION

2-140. Broadcast dissemination allows senders to distribute information simultaneously to a large number of users. Anyone with access to the network can receive the information. The greatest advantage of this method is that information managers can disseminate information to the widest audience in the shortest amount of time. Since the information is sent to a variety of users with varying relevant information requirements, the information cannot be tailored to a specific commander's needs. Another major drawback of broadcast dissemination is that undisciplined use of this method can quickly lead to information overload.

POINT-TO-POINT DISSEMINATION

2-141. Point-to-point dissemination directs information to a specific user or users. Information can be easily passed from one commander to the next. The network can be tailored to meet specific relevant information needs of each recipient with built-in control mechanisms that are not present in broadcast dissemination. Each level of command can filter and integrate information as appropriate and modify it to meet the needs of the next level of command before passing it on. The major disadvantages of point-to-point dissemination are that information reaches a broad audience slowly, and the chances of distortion increase through each level of command.

IDM SCALABILITY

2-142. IDM offers the commander a tremendous amount of flexibility with the capability to configure networks and information systems to meet relevant information needs. Networks can be expanded or contracted to meet the commander’s critical information requirements. Network links can be modified so that throughput is increased or decreased for a particular user. Commanders and staff elements can be designated to receive only certain information and information products. Separate networks can be established to pass only that information which is critical to a particular set of users. Ultimately, IDM allows the commander to determine what information is passed to whom, where, and when.

Chapter 3

Network Operations Roles and Responsibilities

This chapter identifies the organizations and agencies with NETOPS responsibilities that ensure connectivity of network and information systems users throughout the GIG and LWN. It also explains the NETOPS roles and responsibilities of the agencies and network managers at the various levels of the numbered Army, corps, division, BCT, and battalion.

COMMANDER, UNITED STATES STRATEGIC COMMAND

3-1. NETOPS is the operational construct that the CDRUSSTRATCOM will use to operate and defend the GIG. The goal of NETOPS is to provide assured and timely network enabled services across strategic, operational, and tactical boundaries in support of DOD's full spectrum of warfighting, intelligence, and business missions. NETOPS "service assurance" goals include: assured system and network availability, assured information protection, and assured information delivery.

3-2. IAW *Unified Command Plan 02*, Change 2 and the supporting terms of reference, USSTRATCOM will enable and enhance the effectiveness of network defenses by acknowledging and strengthening the close interrelationship between NETOPS and network defense. CDRUSSTRATCOM will act through the CJTF-GNO to—

- Direct operations and defense of the GIG.
- Maintain GIG availability and integrity; ensure efficient traffic management.
- Establish and oversee SA of the GIG readiness and defensive posture.
- Assist the CDRUSSTRATCOM in developing tools, monitoring threats, verifying policy compliance, and controlling network access for consistent IAVM.
- Direct and oversee network defense and information services.
- Assist in establishing and maintaining standards for network, component, and defensive requirements.
- Conduct network defense planning, preparation, and operations employment for normal operations and for crisis and deliberate planning. When directed, support deliberate and crisis action planning requested by other CCDRs.
- Develop, coordinate, integrate, direct, and oversee specific network defense courses of action in support of GIG NETOPS and defense. Coordinate with the CDRUSSTRATCOM for approval authority on Tier 2.1 CND response actions.
- Support USSTRATCOM participation in exercises and experiments involving GIG network management and defense.
- Provide intelligence requirements in support of network defense.
- Provide assessments and recommendations to USSTRATCOM for WATCHCON changes dictated in network threat warning.
- Provide recommendations to USSTRATCOM for INFOCON changes.
- Direct and oversee the establishment and maintenance of standards for technical testing, evaluation, and measures of effectiveness of NETOPS and defense capabilities.
- Direct and oversee establishing procedures to provide department measures of effectiveness and battle damage assessment during and following network defense operations.

- Assist in formulating guidance for training NETOPS and defense forces.
- Assist in developing and promulgating joint tactics, techniques, and procedures for NETOPS and defense activities.
- Identify desired characteristics and capabilities for NETOPS and defense.
- Execute NETOPS through the integration of network and enterprise systems management operations, IA and CND, and IDM/CS into a core GIG operational capability.
- Coordinate with the Chairman of the Joint Chiefs of Staff (CJCS), Services, agencies, combatant commands, and Assistant Secretary of Defense for Networks and Information Integration to develop the policy and CONOPS for collaboratively operating the GIG.
- Establish a global network operations center (GNC) and theater network operations center (TNC) to execute designated responsibilities; provide NETOPS support to theater and functional CCDRs, and coordinate with Services and agencies.
- Establish policies and collaborative procedures that facilitate coordination and information exchange with the other CCDRs, Services and agencies.

Note. Refer to Chapter 4 for additional information on the organizational structure of USSTRATCOM.

COMBATANT COMMANDER

3-3. The CCDR has command and control of the component commands in the assigned theater of operations. This responsibility includes the organizations and systems provided by DOD services and agencies to extend the GIG into the theater. The CCDR's J-6 assumes NETOPS responsibility to manage and control the communications system resources in the joint area.

3-4. The CCDRs, through the supporting role of the NETOPS command and control organizations, exercise OPCON over their portions of the GIG SA information resources (data stores, databases, graphical views, etc.). The combatant command establishes priorities for information collection, filtering, display, dissemination, etc. Consistent with these priorities, the CCDR controls the release of GIG SA information to supporting and multinational forces. Subordinate and supporting commands (service component, functional component, sub-unified commands, and JTF) will provide fault and GND event and performance data on all systems and networks within their commands. On behalf of the CCDR, the NETOPS command and control organizations will consolidate and correlate this data to generate a single integrated GIG SA view that will be available to all organizations via the SIPRNET.

3-5. The theater network operations control center (TNCC) leads the CCDR response to NETOPS events and responds to JTF-GNO direction when required to correct or mitigate a global NETOPS issue. The primary mission of the TNCC is to lead, prioritize, and direct theater GIG assets and resources to ensure they are optimized to support the geographic combatant commander's (GCC's) assigned missions and operations, and to advise the CCDR of the GIG's ability to support current and future operations. The specific roles of the TNCC include monitoring of the GIG assets in their theater, determining operational impact of major degradations and outages, leading and directing responses to degradations and outages that affect joint operations, and directing GIG actions in support of changing operational priorities.

JOINT COMMAND J-6

3-6. The J-6 serves on the CCDRs staff as the communications system director. The J-6 assumes the role of the CCDRs network manager with the establishment of a joint network operations control center (JNCC) that manages and controls all communications systems and networks deployed during joint operations and exercises. The JNCC is the single control agency for the management and operational direction of all joint communications system elements in the theater of operations. The NETOPS responsibilities of the J-6 include:

- Formulating policy and guidance for all communications assets supporting the joint force commander.
- Developing communications system architectures and plans to support the mission of the CCDR.
- Developing policy and guidance for the integration and installation of the operational networks.
- Providing command and control of the joint information systems infrastructure.
- Exercising staff supervision and OPCON of the theater assets provided by DISA, other Services, and other DOD agencies.
- Performing network management activities, functions, and tasks required to effectively and efficiently manage the joint information systems infrastructure and multinational networks supporting the CCDR mission.
- Oversight of the TNCC in the management and control of the CCDRs communications system assets in theater.
- Ensuring adherence to COMSEC principles with the establishment of effective IA program initiatives.

TEMPORARY OPERATIONAL COMMANDS

3-7. At the tactical level, NETOPS functions may be performed by a standing joint force headquarters, standing joint force headquarters CCDR staff combination, combined JTF, or single Service task force. CCDRs may organize a combined JTF or single Service task force and assign tailored forces among the four Service components and special operations forces to the task force commander. The CCDR assigns the task force commander OPCON of designated forces.

JOINT TASK FORCE

3-8. The CJTF will exercise OPCON of the joint force systems and networks through a JNCC as detailed in CJCSM 6231.01C and CJCSM 6231.07D.

ARMY FORCES

3-9. The Army forces (ARFOR) commands and controls the Army Service portion of the JTF. The ARFOR is directly subordinate to the JTF, but is also under the administrative control of the numbered Army to which it is assigned or attached. The ARFOR has a dual NETOPS reporting relationship to the JTF and the geographical combatant command ASCC. The JTF exercises overall authority and responsibility for NETOPS within the ARFOR. The geographical combatant command ASCC also has a responsibility to provide Army-based guidance through technical channels to the ARFOR to ensure compliance with Army modularity and security standards.

3-10. The ARFOR G-6 is the senior signal officer in charge of the Army portion of the JTF information network. The G-6 has the overall responsibility for the information network's responsiveness to supporting the commander's tactical plan.

3-11. The ARFOR role may be filled by a numbered Army, a portion of a numbered Army, a corps or division, or a BCT. Therefore, the exact composition of the ARFOR is highly dependant on the operational scenario. Additional signal assets, such as integrated theater signal battalions/expeditionary signal battalions (ITSB/ESBs), may be attached or assigned to the ARFOR as required.

3-12. The ARFOR G-6 exercises overall authority and responsibility for all NETOPS within the ARFOR AOR. The ARFOR G-6 works closely with the higher headquarters J-6 and subordinate S-6 officers to achieve integrated network management and support services while executing the ARFOR commander's intent. The ARFOR G-6 and staff plan and direct the NETOPS capabilities and support for the ARFOR command posts and provide training and readiness of attached ARFOR assets to ensure efficient and effective mission execution. ARFOR G-6 responsibilities are—

- Recommends communications systems operation network priorities for battle command (e.g., changing bandwidth allocation to support the ARFOR main effort).
- Conducts communications infrastructure management ICW the SC(T) in order to comply with GIG requirements.
- Advises the commander, staff, and subordinate commanders on communications networks and information services.
- Establishes and staffs the G-6's theater communications system information management center.
- Monitors and makes recommendations on all technical communications networks and information services.
- Prepares, maintains, and updates communications systems operation estimates, plans, and orders. Such orders often will cause for CM changes across multiple subordinate elements.
- Provides signal unit operations sections with direction and guidance during preparation of network plans and diagrams establishing the information network.
- Provides signal unit operations sections with unit locations, organizational status, and circuit or data requirements.
- Plans integration of battle command and other information systems.
- Develops, modifies, updates, and distributes signal operating instructions.
- Coordinates with signal offices of higher, adjacent, allied, and coalition units.
- Prepares and publishes SOPs for ARFOR command posts.
- Coordinates, plans, and manages the ARFOR electromagnetic spectrum operational environment, both internal and external, to the Army network within its AOR.
- Plans and coordinates with higher and lower headquarters regarding information systems upgrade, replacement, elimination, and integration.
- ICW the G-2 and the IO officer, performs communications systems operation vulnerability and risk assessments.
- Monitors information dissemination that changes warfighting functions priorities and control measures.
- Coordinates, plans, and directs all IA activities.
- Ensures automation systems and administration procedures for all automation hardware and software employed by the ARFOR are compliant with the GIG procedures and standards or Army LWN specifications.
- Monitors force integration of the force information systems resources.
- Confirms and validates user information requirements in direct response to the tactical mission.
- In concert with the chief of staff or executive officer, establishes and disseminates the electronic battle rhythm.
- Establishes communications system policies and procedures for the use and management of information tools and resources.
- ICW the staff, actively coordinates with a variety of external agencies to develop the information and communications plans, manage the information network, obtain required services, and support mission requirements.

CHIEF INFORMATION OFFICER G-6

3-13. The CIO G-6 provides Army functional policy and guidance regarding NETOPS. The responsibilities of the CIO G-6 are to—

- Develop and resource Army NETOPS policies.
- Approve NETOPS standards ICW the NETCOM/9th SC(A), US Army Signal Center and Fort Gordon, Army Communications-Electronics Life Cycle Management Command, and DISA.
- Develop, maintain, and facilitate sound and integrated IT architecture.

- Integrate the budget, program management, and acquisition decisions affecting information technologies to promote NETOPS inclusion in new information systems.
- Provide policy and guidance on the Army's use of and interface with the Internet, to include Army Web site management.
- Decide overall policy and direction for information systems within the Army.
- Provide the AKO program at http://www.us.army.mil that includes information on IA and the Network Security Improvement Program.

US ARMY SPACE AND MISSILE DEFENSE COMMAND/US ARMY FORCES STRATEGIC COMMAND

3-14. USASMDC/ARSTRAT is the ASCC to USSTRATCOM and directly supports the JTF-GNO. USASMDC/ARSTRAT is also USSTRATCOM's primary point of contact for all Army NETOPS and CND missions. USASMDC/ARSTRAT plans, integrates, and sustains Army CND and is the communications system advocate. The CG, USASMDC/ARSTRAT has designated the CG, NETCOM/9th SC(A) as the USASMDC/ARSTRAT deputy for NETOPS to represent USASMDC/ARSTRAT in communicating and coordinating directly with DOD and USSTRATCOM regarding NETOPS.

UNITED STATES ARMY SIGNAL CENTER & FORT GORDON

3-15. The Commanding General, United States Army Signal Center of Excellence and Chief of the Signal Regiment and Fort Gordon (USASC&FG), directs and supervises all officer and enlisted service school training for the Military Occupational Specialties associated with NETOPS. The United States Army Signal Center of Excellence provides world class Soldiers and Leaders; trains, educates, and develops adaptive IT professionals; and plans, synchronizes, experiments, and implements Future Network capabilities.

3-16. Fort Gordon's 442d Signal Battalion trains Signal Regiment officers (first lieutenant through captain) in order to develop officers with the necessary leadership, technical and tactical skills to support the Army and Joint forces. The courses trained by the 442d Signal Battalion are:

- Signal Basic Officer Leader Course Phase III—teaches communications planning and management; communications interface; leadership; information technology; electronics; microwave; tropospheric scattering; property accounting; telecommunications; COMSEC accounting; training management; military justice; signal systems tactics and doctrine. The course also includes communications requirements, planning and execution unique to a maneuver battalion or brigade.
- Signal Captains Career Course—provides US Army signal officers the academic instruction, which supports the leader, tactical, and technical skills needed to lead company-size units and to serve at battalion and brigade staff levels.
- Signal Captains Career Course-Reserve Component—provides Reserve Component signal officers with technical updates related to:
    - Communications interfaces.
    - Electronic warfare.
    - Chemical, biological, radiological and nuclear operations.
    - Leadership.
    - Human resources support.
    - Property accounting.
    - Training management.
    - Force integration.
    - Military justice.
    - Signal system tactics and doctrine.

- Battalion Command, Control, Communications, and Computer Operations Staff Officer (S-6) Course—utilizes the Signal Captains Career Course knowledge as a foundation. The S-6 course provides small group instruction heavily reliant upon hands-on learning and practical exercise. The goal of the course is to produce signal staff officers with the skills required to plan a signal communications network, produce an Annex H (signal annex), and manage the implementation and troubleshooting of combat net radio, Army Battle Command System, and command post node networks. There are no prerequisites for this course. However, the course requires either pre-existing knowledge of combat net radio or completion of distance learning products to allow the content of the instruction to reach the higher levels of knowledge. The course content includes:
    - Administration (Skills Assessment Exam, assigned homework and computer based tutorials).
    - Military decision making process and planning tools (Systems Planning, Engineering, and Evaluation Device/Terrain Analysis).
    - Spectrum management and electronic warfare.
    - Antenna theory.
    - S-6 management (unit standing operating procedures, SMART books, battery management plans).
    - Very high frequency-frequency modulation, Defense Advanced Global Positioning System Receiver, Simple Key Loader.
    - High frequency and automatic link establishment planning (AN/PRC-150).
    - Multi-band radio planning (AN/PSC-5C, AN/PRC-117).
    - Handheld radios (AN/PRC-148 [Multiband Inter/Intra Team Radio], AN/PRC-152).
    - Force XXI Battle Command, Brigade-and-Below.
    - Command post node networks.
    - Tactical Information Management System, Lower Tactical Internet, Enhanced Position Location and Reporting System.
    - Army Battle Command System integration exercise.
    - CAPSTONE exercise.
    - Advanced technology briefings.

3-17. The 442d Signal Battalion's purpose is to prepare signal corps company grade officers for company level command and for assignments to staff positions at battalions and brigades, both signal and non-signal, with primary emphasis on signal operations.

3-18. The 442d Signal Battalion is part of the Leader College of Information Technology at USASC&FG and information on signal officer education and training can be obtained by contacting the Chief, Officer Education and Training Division at (Commercial) (706) 791-2150 or (DSN) 780-2150.

3-19. Personnel interested in attending a 442d Signal Battalion or noncommissioned officer Academy Course should contact their branch/functional area representative, local post/installation training coordinator for Army Training Resources and Requirements System enrollment or the 442d Signal Battalion, Training Support Division at (Commercial) (706) 791-0192 or (DSN) 780-0192.

CAPABILITIES DEVELOPMENT INTEGRATION DIRECTORATE

3-20. The Capabilities Development Integration Directorate/TRADOC Integration Office (CDID/TIO)-Networks is responsible for managing and integrating the user activities associated with the development, synchronization, and integration of Communications Networks and associated aspects of the Army. The CDID/TIO-Networks will manage the commonality and interoperability aspects within the current and future force to ensure Army, Joint, Interagency, and Multinational interoperability. CDID/TIO serves as user representative for all aspects of the communications network system of systems. Intensively manage

and synchronize all organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) actions in order to deliver network capabilities over time. CDID/TIO is responsible for capabilities development and support of system testing and fielding. Oversee efforts that implement and update the LandWarNet transition strategy for current force network transport and operations. In addition, CDID/TIO is responsible for the three TRADOC Capabilities Managers (TCM), the Experimentation Division, and the Signal Concepts, Requirements, and Doctrine Division.

TRADOC PROJECT OFFICE DIRECTOR FOR NETWORK OPERATIONS

3-21. TRADOC Project Office (TPO) NETOPS, reporting to the SIGCEN Commanding General as an integral part of the CDID, will perform as the Army's primary focal point as a user advocate for the integration and synchronization activities associated with functional capability area Network Operations and Electro-Magnetic Spectrum Operations (EMSO). TPO NETOPS is responsible for the integration and synchronization of all systems or components of systems designated as performing NETOPS functions, EMSO, and Communications Security (COMSEC). The TPO Director acts for the proponent in discharging responsibilities in developing and integrating total system requirements in the area of Network Operations and EMSO. In this capacity, TPO NETOPS, as part of the CDID, is the counterpart to TRADOC Capabilities Manager (TCM) Networks & Services (N&S), TCM - SATCOM & Network Extension (SNE), and TCM Tactical Radio (TR). TPO NETOPS is a user advocate responsible for coordinating integration efforts across key programs of record such as the Warfighter Information Network -Tactical (WIN-T), Joint Tactical Radio System (JTRS), Battle Command systems, and Future Combat System (FCS).

3-22. TPO NETOPS is responsible for duties as outlined in TRADOC Regulation 71-12, TRADOC System Management. The TPO will coordinate with the appropriate TCMs and other organizations to ensure that all doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) imperatives are developed and synchronized with respect to the fielding of NETOPS capabilities and associated systems. The TPO will coordinate to ensure that existing programs of record are appropriately modified in providing materiel solutions.

NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND (ARMY)

3-23. NETCOM/9th SC(A) is the Army's CONUS-based, worldwide network and systems provider. It supports the Army's force projection mission through its integrated, worldwide-deployable theater tactical units, strategic and sustaining-base units, and global network operations role. As the executive agent for the Army's portion of the GIG, NETCOM/9th SC(A) exercises network and information systems control at the strategic and operational military operations. It also executes the strategic and sustaining-base and theater tactical communications systems integration with all Service components, defense agencies, and nongovernmental organizations. Refer to FMI 6.02-45 for additional information on NETCOM/9th SC(A) theater tactical units. The NETOPS responsibilities include:

- Establishing and enforcing theater and Army NETOPS policies and procedures for the LWN.
- Providing input for the JTA-A, JTSSNMCCB, and Installation Information Infrastructure Architecture Configuration Control Board.
- Providing a centralized configuration control capability to monitor and manage configuration changes of Army tactical and strategic voice and data switches.
- Serving as the Army's primary interface with the DISA on issues related to the performance of DISA-managed long-haul networks.
- Providing NETOPS for the LWN and NETOPS support to ACOMs and DOIMs.
- Providing command and control for the primary Army organizations performing NETOPS at the enterprise level in CONUS and at all other levels.
- Performing Army ESM/NM activities, functions, and tasks during exercises and operations of peacetime and war.

- Managing the Army Internet domain (.mil or .smil) as the Army's Internet Service Provider and manager.
- Operating provisions and equipping the A-GNOSC and the TNOSCs.
- Providing operation and maintenance and Army ESM/NM for networks and information systems under its direct responsibility.
- Providing an IA program to unify the Army's ESM/NM and information security functions.
- Exercising CM of the integrated hardware and software solutions for the Army's WAN and systems security infrastructure.
- Providing an IDM capability for network and information system users.

ARMY GLOBAL NETWORK OPERATIONS AND SECURITY CENTER

3-24. The A-GNOSC mission is to provide Army and DOD NETOPS reporting and situational understanding for the LWN. The A-GNOSC provides worldwide operational and technical support to the LWN across the strategic, operational, and tactical levels. The A-GNOSC interfaces with all Army TNOSCs, functional NOSCs, the DISA GNOSC, as well as other Service's NOSC. The A-GNOSC will—

- Carry out performance management (monitoring and analyzing) of tactical Army networks.
- Provide network and systems administration of lower echelon Army NOSCs.
- Receive and coordinate requests for services that cross regional boundaries.
- Design, operate, and manage the Army's protected DNS—the Army's world-wide "electronic address book."
- Operate and manage data storage and retrieval for enterprise-level applications hosted on AKO or consolidated servers.
- Manage the enterprise-level architecture for the Army's directory services (e.g., Microsoft Windows 2000) and AD enterprise-level architecture. The AD enterprise-level architecture includes domain management of all consolidated Windows 2000 domains and domain controllers.
- Provide technical guidance to installations and sites for migration to Windows 2000 and AD.

THEATER NETWORK OPERATIONS AND SECURITY CENTER AND REGIONAL NETWORK OPERATIONS AND SECURITY CENTER

3-25. The TNOSC mission is to act as the single point of contact for Army network services, operational status, and anomalies in the theater. The TNOSC provides visibility and status information to the A-NOSC and TNC. In some theaters, the TNOSC may provide visibility to other Service component NOSCs. There are TNOSCs established in all theaters of operations: CONUS, Europe, Pacific, Korea, and Southwest Asia.

3-26. These TNOSC functions are interchangeable across all theaters. Theater common functions can be performed at multiple geographical locations and should be performed the same way at each location.

3-27. The TNOSC will perform or coordinate any task that spans the theater or multiple regions. This will provide consistent service among regions. It will also place the operational function at the only location in the enterprise that would have visibility or awareness of what was happening in both regions. The TNOSC will—

- Provide additional event management capabilities such as analysis and correlation of event data, to the tactical units, as required.
- Build, test, and provide software distribution packages to the tactical units.
- Perform performance management (monitoring and analyzing) of the tactical units' systems.
- Prepare and implement COOP in support of the tactical units.
- Exercise, monitor, and evaluate COOP in support of the tactical units.
- Determine system patch implementation.
- Determine if the patch requires testing.

- Notify the A-GNOSC of the impending patch.
- Coordinate and direct patch implementation.
- Notify the DOIM, regional service center, RNOSC, and the tactical units of the impending patch.
- Build the patch package.
- Conduct necessary patch testing.
- Perform global address list synchronization for the tactical units.
- Manage e-mail hubs in support of the tactical units.
- Provide technical support on problems escalated from the DOIM for tactical units.

3-28. The RNOSC performs NETOPS functions that provide strategic, reach operations, and operational environment information and network service to support CCDRs, organizations, and agencies within the assigned AOR. The RNOSC supports operations and maintenance of RNOSC-level LWN related information systems and services and network management, IA, and IDM functions within its area of operation. The RNOSC is the single point of coordination for end-to-end connectivity to the GIG and LWN infrastructure for the CCDR it supports.

SIGNAL COMMAND (THEATER)

3-29. The SC(T) provides NETOPS capabilities and support to theater, joint, and coalition forces. These forces leverage the LWN to enable extension and reach operations capabilities in support of the CCDR. It operates the LWN in the numbered Army AOR and provides assured delivery of common user services in support of the CCDR and the numbered Army. With additional joint manning document-based augmentation, the SC(T) may also assume joint and coalition NETOPS functions for a CJTF or combined joint force land component command.

3-30. The SC(T) consists of all strategic- and operational-level signal organizations within the theater of operations. It plans, installs, operates, manages, controls, and maintains data, voice, and video networks and information systems throughout the theater. The SC(T) performs centralized NETOPS activities for the networks that provide communications capabilities to the ASCC, ARFOR, and joint forces in the JTF AOR. The SC(T) is a major subordinate command of the NETCOM/9th SC(A). Under the OPCON of the ASCC, the SC(T) commander is dual hatted as the ASCC G-6.

3-31. The SC(T) performs various tasks depending on the military operation or situation. The CCDR may task the SC(T) to provide overall signal command and control, direction, and guidance to a JTF or assign portions of the signal mission to the SC(T). All or a portion of the SC(T) may be tasked to establish or augment the JNCC when the numbered Army and ASCC is tasked as the JTF, or provide land forces network control when tasked to act as a JFLCC or ARFOR. In these scenarios the JNCC and JFLCC NOSC report directly to the CCDR J-6.

3-32. The SC(T) is comprised of one or more signal brigades (tactical), a signal brigade (strategic), and a TNOSC, and it may have a combat camera company and/or a tactical installation and network company assigned as depicted in Figure 3-1. The SC(T) NETOPS responsibilities include:

- Providing centralized management control and engineering for the Army Theater's data, voice, and video networks. This includes network interfaces with joint, combined, and coalition systems.
- Operating a fixed TNOSC during normal strategic operations of the LWN, and a deployed NOSC during tactical operations.
- Formulating and implementing plans, policies, and procedures for the engineering, installation, operation, management, and control of assigned portions of the LWN.
- Providing network planning and management of special purpose communications and information systems.
- Providing IA planning and management for the theater networks and information systems.
- Providing an IDM capability for network and information systems users in the theater.

- Establishing or augmenting the JNCC as required and staffing the Army's portion with augmentation from other Services.
- Providing frequency assignments for Army, joint, and coalition elements throughout the theater.
- Providing planning and staff management of the ground mobile forces tactical satellite in the theater of operations.

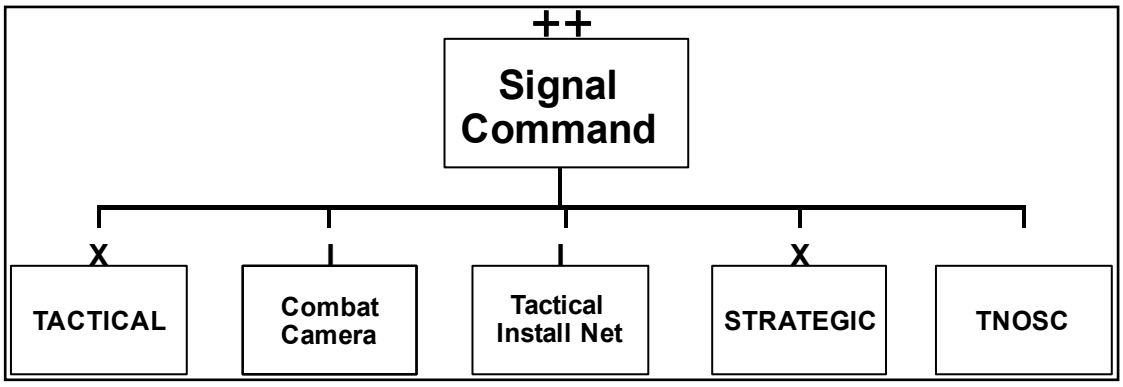

Figure 3-1. SC(T) structure

3-33. The SC(T) TNOSC NETOPS responsibilities include:

- Operating TNOSCs and providing guidance through technical channels to Army NOSCs within the theater at all echelons.
- Supervising the operation of NETOPS tools such as the AENIA standard tool capabilities, Integrated Systems Control (ISYSCON), and IA management assemblage. (Refer to Appendix B for more information on these and other NETOPS tools.)
- Exercising OPCON of other communications assets provided by external organizations and agencies.
- Managing all signal support interfaces with joint and multinational forces, including host nation support interfaces.
- Managing and controlling the LWN and network services from the strategic force projection sustaining base to the tactical units.
- Performing ESM/NM activities, functions, and tasks required to effectively and efficiently manage the information systems infrastructure and multi-organizational networks supporting the operational mission.
- Ensuring the IA tools are in place to provide security integrity of the network, protection for the network and support secure access controls and connectivity.

SIGNAL BRIGADE (STRATEGIC)

3-34. The signal brigade (strategic) provides fixed, strategic communications support to the Soldier. Each strategic signal brigade is unique and tailored to support specific theater requirements. The TNOSC supports the strategic signal brigade in performing NETOPS functions for the networks and information systems that support an ongoing presence in the theater. These functions include backbone networks, e-mail, frequency assignment, circuitry, gateway routing to multinational networks, and commercial and Defense Switched Network (DSN) access out of the theater of operations. During peace, each CONUS strategic signal brigade is doctrinally under the command and control of the NETCOM/9th SC(A). During major theater war or peacetime operations, the SC(T) assumes OPCON of the brigades deploy from CONUS or other theaters of operations.

SIGNAL BRIGADE (TACTICAL)

3-35. The OCONUS signal brigade (tactical) (SB[T]) provides tactical communications support capability to the numbered Army and ASCC. The signal brigade tactical is doctrinally under the command and control of the SC(T). The SB(T) deploys to provide tactical communications systems operation support to the ASCC. The brigade will also assume command and control of any assigned or attached signal unit and install, operate, and maintain assigned portions of the theater communications network as directed. The brigade S-3 will establish a tactical NOSC to perform the NETOPS functions required to manage and control the networks and information systems it provides in the theater.

3-36. In an operational scenario, elements of the tactical signal brigade may be placed under the OPCON of various operational commands such as a JTF, JFLCC, and JTF ARFOR, corps, division, or brigade. SB(T) assets are also commonly placed under the OPCON of operational elements in a remote theater when required. (Refer to FMI 6-02.45 for additional information on SC(T), and the supporting units.)

INTEGRATED THEATER SIGNAL BATTALION

3-37. The centerpiece of the current force transformation of theater tactical signal units is the ITSB/ESB. The ITSB/ESB is organized into multifunctional elements, each containing all of the switching equipment, the transmission systems, the data network management systems, and the command and control and data network management resources that comprise a complete signal node.

3-38. The multifunctional nodal structure of the ITSB/ESB reflects a train-as you-fight and organize-as-you-fight philosophy. This alleviates one of the greatest difficulties of the current structures, which is to task organize from multiple organizations to form a single communications node in order to support a single customer enclave.

3-39. The ITSB/ESB will typically be assigned to a SB(T), although it may be assigned or attached to other organizations as well.

3-40. The ITSB/ESB and its subordinate companies are multifunctional organizations that are designed in a modular fashion. Modules are designed around communications nodes so that support to the customer can be easily tailored in a scalable fashion by deploying the required number of nodes.

3-41. Each node module includes voice switching and data networking capabilities, along with a mixture of transmission systems such as SATCOM, tropospheric scatter, and line of sight.

EXPEDITIONARY SIGNAL BATTALION

3-42. The ESB is being created to addresses shortcomings in ITSB capabilities. At the same time, the highly modularized ESB structure will serve as an organizational platform into which Warfighter Information Network-Tactical capabilities can be introduced with minimal adjustment.

3-43. Outdated mobile subscriber equipment switching and line of sight systems employed by the ITSB do not meet the data throughput requirements of supported units at any echelon. The ESB incorporates the next generation of switch/data systems. Joint Network Transport Capability-Spiral capabilities, such as the joint network node (JNN) and command post node (CPN), can provide the needed data capacity at all levels and network services consistent with those provided to Soldiers at corps and division levels. The ESB will also serve as an organizational platform for the introduction of Warfighter Information Network-Tactical capabilities as they become available. The ESB is dependent on the fielding of the Joint Network Transport Capability-Spiral or Warfighter Information Network-Tactical systems to completely equip the unit.

3-44. Replacement of mobile subscriber equipment systems will greatly enhance the maneuverability of supported units and improve compatibility with corps- and division-level units. The ability to relocate a command post quickly with minimal network installation and tear-down times will be especially important to functional battalions supporting division-level organizations in a fast-moving operation.

3-45. Introduction of the next generation switch/data systems and a reduction in the number of large switches will allow the battalion to be structured in a way that better enables employment of network assets

to support the increased number of medium and small command posts. This flexible structure will improve the battalion's ability to respond quickly to support missions with precisely-sized capabilities, down to team level, that minimize the deployed signal footprint. The total support capability of the ESB grows from 27 to 30 command posts.

DIRECTOR OF INFORMATION MANAGEMENT

3-46. The DOIM provides overall NETOPS for the data and voice networks and Army information systems on their base, post, camp, and station or within an assigned geographical area. Under ACOM guidelines and procedures, DOIMs plan and budget for appropriate network and information systems hardware and software technology upgrades or replacements to ensure that customer demands are met. They work with external organizations to ensure the proper operation of installation-level components of DOD or Army-level networks and information systems. The DOIM NETOPS responsibilities include:

- Managing all support functions associated with providing customer access to the installation common-user networks and information systems infrastructure.
- Ensuring support and problem resolution for physical networks and information systems equipment that provide access to DOD or Army-level networks and information systems.
- Sharing information with other network managers concerning lessons learned and innovative ideas to support users.
- Implementing NETOPS practices IAW DOD, Army, information management activity, and RCIO policy and guidance.
- Establishing policies and procedures for the performance of the operation and maintenance of networks and information systems within its AOR.
- Establishing Service level support agreements with the NETCOM/9th SC(A).
- Coordinating with RCIO and NETCOM/9th SC(A) for management of inter-installation networks and information systems that affect their supported organizations.
- Establishing and managing the command IA program for base, post, camp, and station. OCONUS, this function is provided by the signal battalions.
- Using NETOPS activities, functions, and capabilities to effectively and efficiently manage the use of the network and information system resources within its AOR.
- Providing mission impact of outages, CND incidents, and other network issues to the TNOSC.
- Responding to TNOSC direction in support of problem resolution, change requests, and IAVMs.

3-47. DOIMs are organic elements of the United States (US) Army Garrison. While DOIMs report directly to their Garrison Commander, NETCOM/9th SC(A) manages the CONUS DOIMs' technical functions through their RCIO, who is co-located with the Installation Management Command regional headquarters.

3-48. NETCOM RCIOs are OPCON to Installation Management Command region directors and serve as the G-6 for the region. They focus on day-to-day network related issues and develop and enforce network architectures, programs, IT budgets, policies, and standards. There are three CONUS RCIOs located at Fort McPherson, Georgia; Fort Sam Houston, Texas; and Fort Monroe, Virginia. There are three OCONUS RCIOs located in Heidelberg, Germany; Yongsan, Korea; and Fort Shafter, Hawaii, designated from theater signal commands.

G-6, S-6, AND SIGNAL UNIT S-3

3-49. The S-3 serves as the strategic or tactical signal unit's operations officer, and the G-6 or S-6 serves as a non-signal unit's communications systems operation officer depending on the unit's structure and level of responsibility. In all cases, the S-3, G-6, and S-6 work in concert to conduct NETOPS in their AOR. The S-3, G-6, and S-6 ensure that data and voice networks and information systems are available and secure for commanders to receive the information they need to command and control their forces throughout an area of operations. (Refer to FM 5-0.1 for additional information on the operations process of the S-3, G-6, and S-6.)

3-50. The numbered Army is the ASCC for the theater. Numbered Army organic signal support consists of the numbered Army G-6 staff and the SC(T). The numbered Army G-6 has duel responsibilities as the commander of the SC(T). The NETOPS responsibilities of the G-6 at numbered Army or ASCC include:

- In conformance with Army global and theater NETOPS policies, establish NETOPS policies and procedures for the integration, installation, and operation and maintenance of the operational networks under their direct responsibility.
- Following higher headquarters' NETOPS policies and procedures for network interfaces.
- Coordinating all communications systems operation support interfaces with joint and multinational forces, including host nation support interfaces.
- Coordinating the availability of commercial information systems and services for military use.
- Exercising staff supervision of other communications assets provided by external organizations and agencies.
- Managing communications protocols through the coordination of DISN and tactical network user interfaces down to the battalion Tactical Internet.
- Planning redundant signal means to pass time-sensitive battle command information from collectors to processors.
- Managing the employment automation (hardware and software) supporting the force, including the operations of the automation management office.
- Establishing automation systems administration procedures for all automation software and hardware employed by the force.
- Establishing information systems security policy for all automation software and hardware employed by the force.
- Establishing IA policies and procedures for the command and enforcing command global policies.
- Providing supporting assets and services to deployed and deployable units.
- Responding to TNOSC direction in support of problem resolution, change requests, and IAVMs.
- Ensuring and reporting IAVM compliance for all IT networks, systems and devices.
- Performing organizational level maintenance on unit communications and electronic systems, remote control systems, intercoms, information systems and other battlefield functional area systems.
- Troubleshooting to a defective line replaceable unit (LRU)/line replaceable module (LRM) unit communications and electronic systems, remote control systems, intercoms, information systems and other battlefield functional area systems.
- Replacing and evacuating to the forward support company for repair of faulty LRUs/LRMs on communications and electronic systems, and information systems.
- Repairing and installing unit communications and electronics systems wiring and cabling.
- Performing the installation and removal of all unit vehicular and base station communications, electronics, and information systems.
- Performing communications and electronic systems test using appropriate test, measuring and diagnostic equipment (TMDE). Maintains TMDE calibration records.
- Managing and maintaining battery inventory and charging systems.
- Ordering and maintaining bench stock.

TACTICAL NETWORK OPERATIONS

3-51. The G-6 has the overall responsibility for the corps and division information network's responsiveness to supporting the commander's tactical plan. Figure 3-2 outlines network responsibilities for the division staff operations cell. The same responsibilities are applicable at the corps.

3-52. The corps and division consist of an organic headquarters element which commands maneuver and support elements that have been assigned to meet mission requirements. Corps and division signal support

consists of the signal corps or division G-6 cell and a corps or division signal company. Additional signal assets, such as ITSB/ESB, may be attached or operationally controlled to the corps and division as required.

3-53. The corps and division G-6 exercises overall authority and responsibility for all NETOPS within the AOR IAW Army and theater policies and procedures. The G-6 may also be required to serve as the Army component signal commander or joint command signal commander. The corps and division G-6 works closely with the higher headquarters G-6, J-6, subordinate S-6 officers, and the corps and division signal company to achieve integrated network management and support services while executing the commander's intent. The corps and division G-6 and staff plan and design the NETOPS capabilities and support for the command posts and subordinate units, as well as providing training and readiness responsibility to ensure efficient and effective mission execution for assigned and attached units.

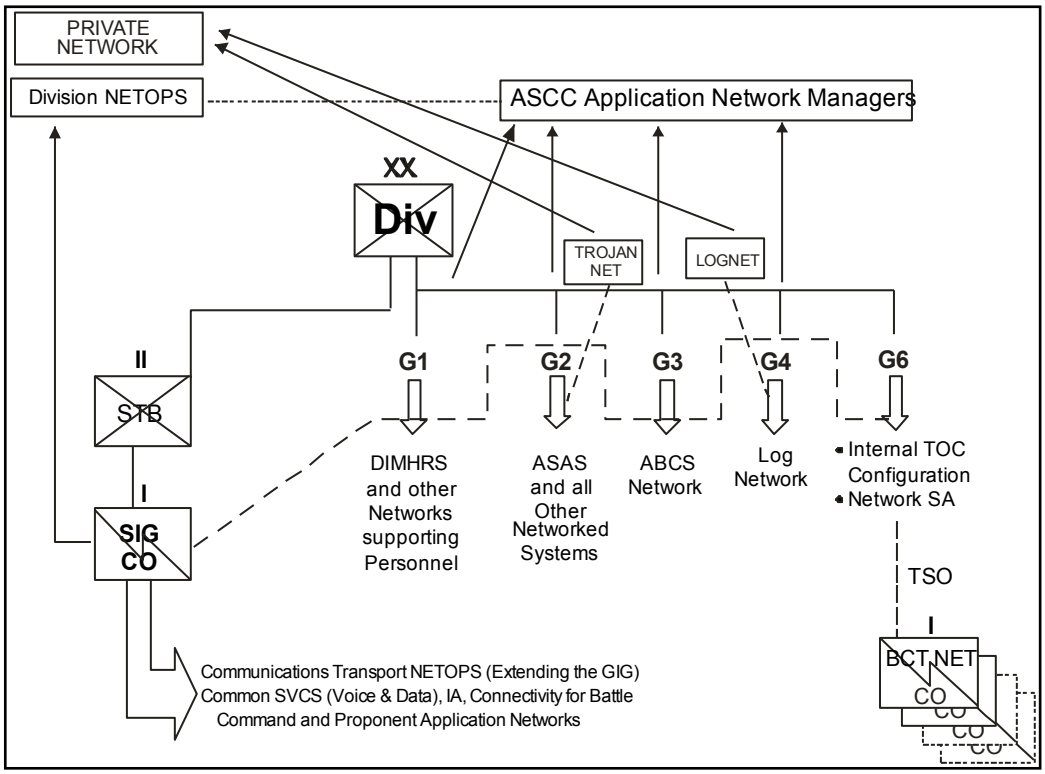

Figure 3-2. Division network responsibilities

3-54. The corps and division habitually provide AOR services from the forward-deployed corps or division tactical operations center (TOC). Due to recent enhancements to tactical reach operations capability, the corps and division G-6 may elect to stage select services from remote sanctuary locations. These locations include the corps and division tactical unit hub node (UHN) or a corps and division-controlled cell within the network service center regional. Staging corps and division services at sanctuary locations is generally most effective during deployment and decisive operations. During these phases, the corps and division TOCs are highly mobile and are unable to provide a stable, high-speed environment to host AOR services. The corps and division G-6 has the following responsibilities:

- Recommends communications systems operation network priorities for battle command (e.g., changing bandwidth allocation to support the corps and division main effort: a BCT reinforced with additional intelligence, surveillance, and reconnaissance assets).
- Conducts IT infrastructure management ICW the numbered Army SC(T) in order to comply with GIG requirements.
- Acts as the Army component G-6 when needed (equipment and personnel augmentation will be required to support this mission).

- Acts as the JTF J-6, if required. Equipment and personnel augmentation will be required to support this mission and will be provided by the numbered Army or ASCC as necessary.
- Advises the commander, staff, and subordinate commanders on communications networks and information services.
- Supervises the activities of the NETOPS officers and units NETOPS activities.
- Monitors and makes recommendations on all technical communications networks and information services.
- Prepares, maintains, and updates communication systems operation estimates, plans, and orders. Such orders often will cause for CM changes across multiple divisions.
- Provides signal unit operations sections with direction and guidance during preparation of network plans and diagrams establishing the information network.
- Provides signal unit operations sections with unit locations, organizational status, and circuit or data requirements.
- Works issues on information systems equipment and personnel requirements analysis due to the modified table of organization and equipment changes.
- Plans integration of battle command and other information systems.
- Develops, modifies, updates, and distributes signal operating instructions.
- Coordinates with signal offices of higher, adjacent, allied, and coalition units.
- Prepares and publishes communications systems operation SOPs for corps and division command posts.
- Coordinates, plans, and manages the electro magnetic spectrum operational environment, both internal and external, to the corps and divisions within its AOR.
- Plans and coordinates with higher and lower headquarters regarding information systems upgrade, replacement, elimination, and integration.
- ICW the G-2 and the IO officer, performs communications systems operation vulnerability and risk assessments.
- Monitors information dissemination that changes warfighting function priorities and control measures.
- Coordinates, plans, and directs all IA activities.
- Ensures that automation systems and administration procedures for all hardware and software employed by the corps and division are compliant with the GIG procedures and standards or Army specifications policies.
- Monitors force integration of the force information systems resources.
- Confirms and validates user information requirements in direct response to the tactical mission.
- ICW with the chief of staff or executive officer, establishes and disseminates the electronic battle rhythm.
- Establishes communications system policies and procedures for the use and management of information tools and resources.
- ICW the staff, actively coordinates with a variety of external agencies to develop the information and communication plans, manages the information network, obtains required services, and supports mission requirements.
- Plans, manages, and directs all IA activities ICW the TNOSC and RCERT.
- ICW the G-6 staff, plans and designs the NETOPS capabilities and support for the corps and division command posts and subordinate units. They also provide training and readiness responsibility to ensure efficient and effective mission execution.
- Performing organizational level maintenance on unit communications and electronic systems, remote control systems, intercoms, information systems and other battlefield functional area systems.

- Troubleshooting to a defective line replaceable unit (LRU)/line replaceable module (LRM) unit communications and electronic systems, remote control systems, intercoms, information systems and other battlefield functional area systems.
- Replacing and evacuating to the forward support company for repair of faulty LRUs/LRMs on communications and electronic systems, and information systems.
- Repairing and installing unit communications and electronics systems wiring and cabling.
- Performing the installation and removal of all unit vehicular and base station communications, electronics, and information systems.
- Performing communications and electronic systems test using appropriate test, measuring and diagnostic equipment (TMDE). Maintains TMDE calibration records.
- Managing and maintaining battery inventory and charging systems.
- Ordering and maintaining bench stock.

Note. Appendix D provides division commanders and staff members an understanding of systems and personnel that comprise the communications network at division.

BRIGADE COMBAT TEAM AND SUPPORT BRIGADE

3-55. The modular design of Army tactical forces employs six basic types of brigade-sized formations: the BCT and five support brigades. The BCT is a standing combined arms formation intended to conduct close combat in offensive, defensive, and stability operations. The other five types of tactical brigades will perform supporting functions and include a battlefield surveillance brigade, a combat support brigade, a fires brigade, a combat aviation brigade, and a sustainment brigade. Organic signal support includes a signal company. In addition, the brigade S-6 possesses a small team of embedded signal Soldiers.

3-56. Any tactical brigades, tactical companies, and other tactical units which do not possess an organic signal company will be supported via pooled numbered Army or ASCC tactical signal assets. The NETOPS functions of these units are addressed under the category of ITSB/ESB supported echelons.

Brigade and Brigade Combat Team S-6 Responsibilities

3-57. On behalf of the commander, the brigade S-6 maintains overall authority and responsibility for all NETOPS within the brigade AOR in compliance with joint, Army, and theater policies. The brigade S-6 may also be required to serve as the Army component signal commander. The brigade S-6 works closely with its higher headquarters G-6, J-6, and the brigade signal company to achieve integrated NETOPS while executing the brigade commander's intent.

3-58. The brigade S-6 and staff plan the NETOPS capabilities and support (e.g., voice, video, networks, messaging) for the brigade command posts and subordinate units. The S-6 section personnel are located within brigade command posts to support the commander's identified NETOPS requirements. The brigade and BCT S-6—

- Recommend communications system network priorities for battle command (e.g., changing bandwidth allocation to support the BCT main effort: a maneuver battalion reinforced with additional intelligence, surveillance, and reconnaissance assets).
- Conduct communications infrastructure management in conjunction with the numbered Army SC(T) to comply with GIG requirements.
- Act as the Army component G-6 when needed. Equipment and personnel will be required to support this mission. Equipment will be provided by the corps, division, and numbered Army.
- Advise the commander, staff, and subordinate commanders on communications networks and information services.
- Plan, configure, manage, and monitor the TOC LAN and Tactical Internet for all brigade command posts.

- Supervise the activities of the NETOPS cell.
- Monitor and makes recommendations on all technical communications networks and information services.
- Prepare, maintains, and updates communications systems operation estimates, plans, and orders. They also coordinate such efforts with the higher headquarters' G-6, J-6, and signal company.
- Provide the brigade NOSC with direction and guidance during preparation of network plans and diagrams, establishing the information network.
- Provide signal unit operations sections with unit locations, organizational status, and circuit or data requirements.
- Work issues on information systems equipment and personnel requirements analysis due to modified table of organization and equipment changes.
- Plan integration of battle command and other information systems.
- Develop modify, update, and distribute signal operating instructions.
- Coordinate with signal offices of higher, adjacent, allied, and coalition units. Prepares and publishes communications systems operation SOPs for brigade command posts. Plans and coordinates with higher and lower headquarters regarding information systems upgrade, replacement, elimination, and integration. The brigade and BCT S-6 are responsible for all network assets IAW joint, Army, and theater policy.
- Perform communications systems operation vulnerability and risk assessments ICW the BCT S-2 and the IO officer.
- Monitor information dissemination that changes warfighting function priorities and control measures.
- Coordinate, plans, and directs all IA activities (AR 25-2 and unit SOP provide details on IA activities).
- Ensure that automation systems and administration procedures for all automation hardware and software employed by the brigade are compliant with the GIG procedures and standards or Army specifications.
- Confirm and validates user information requirements in direct response to the tactical mission.
- Perform all of the duties and responsibilities of the corps and division G-6 when the brigade is operating independently.
- Coordinate, plan, and manage the electro magnetic spectrum operational environment, both internal and external, to the brigade within its AOR.
- Plan and manage the brigade information network ICW the operational chain of command.
- Plan and manage brigade IA systems (firewalls, IDSs, and ACLs) ICW the TNOSC.
- Plan and manage brigade IDM/CS procedures (user profiles, file and user priorities, and dissemination policies).
- Deploy range extension assets to maintain connectivity and reliability of the brigade communications network.
- Evaluate network requirements to determine needs for unmanned aerial vehicles and communications relay requirements.
- Execute command and control of all NETOPS responsibilities in support of the unit mission.
- Performing organizational level maintenance on unit communications and electronic systems, remote control systems, intercoms, information systems and other battlefield functional area systems.
- Troubleshooting to a defective line replaceable unit (LRU)/line replaceable module (LRM) unit communications and electronic systems, remote control systems, intercoms, information systems and other battlefield functional area systems.
- Replacing and evacuating to the forward support company for repair of faulty LRUs/LRMs on communications and electronic systems, and information systems.

- Repairing and installing unit communications and electronics systems wiring and cabling.
- Performing the installation and removal of all unit vehicular and base station communications, electronics, and information systems.
- Performing communications and electronic systems test using appropriate test, measuring and diagnostic equipment (TMDE). Maintains TMDE calibration records.
- Managing and maintaining battery inventory and charging systems.
- Ordering and maintaining bench stock.

Note. Appendix E provides BCT commanders and staff members a brief overview of the related mission responsibilities of the S-6. Similar to the division, the BCT is required to operate its own network without augmentation from higher headquarters.

BRIGADE SIGNAL COMPANY

3-59. The brigade has an organic signal company to provide NETOPS capabilities and support. The brigade signal company is comprised of a NETOPS cell and two network extension platoons, as depicted in Figure 3-3. The brigade signal company contains many of these same components while it is tailored to the requirements of a specific support brigade. In general, the NETOPS capabilities in the signal company are resourced to support connectivity to the enterprise LWN services; operate, manage and defend NETOPS assets in its AOR; and extend strategic NETOPS policies into the tactical formation. The signal company maintains organic network systems and devices. Signal soldiers are designated operator/maintainer for major network assemblages.

Brigade Network Service Support Locations

3-60. The brigade habitually provides network services from the forward-deployed brigade command post. Due to recent enhancements to tactical reach operations capability, the brigade S-6 may elect to stage select brigade services from numbered Army-hosted strategic sanctuary locations, such as a network service center regional. Staging brigade services at sanctuary locations is generally most effective during deployment and decisive operations. During these phases, the brigade command post is highly mobile and is unable to provide a stable high-speed environment to host network services.

MANEUVER AND SUPPORT BATTALIONS

3-61. Battalions possess an organic signal capability consisting of a signal officer (S-6) and staff; additional signal assets may be attached or assigned as required. As part of Army transformation, battalions are fielded with new technologies (e.g., satellite access provided by the Joint Network Transport Capability) to extend the LWN into the tactical formation.

Note. A force design update has been submitted to move the NETOPS cell from within the signal company to the G-6/S-6 section.

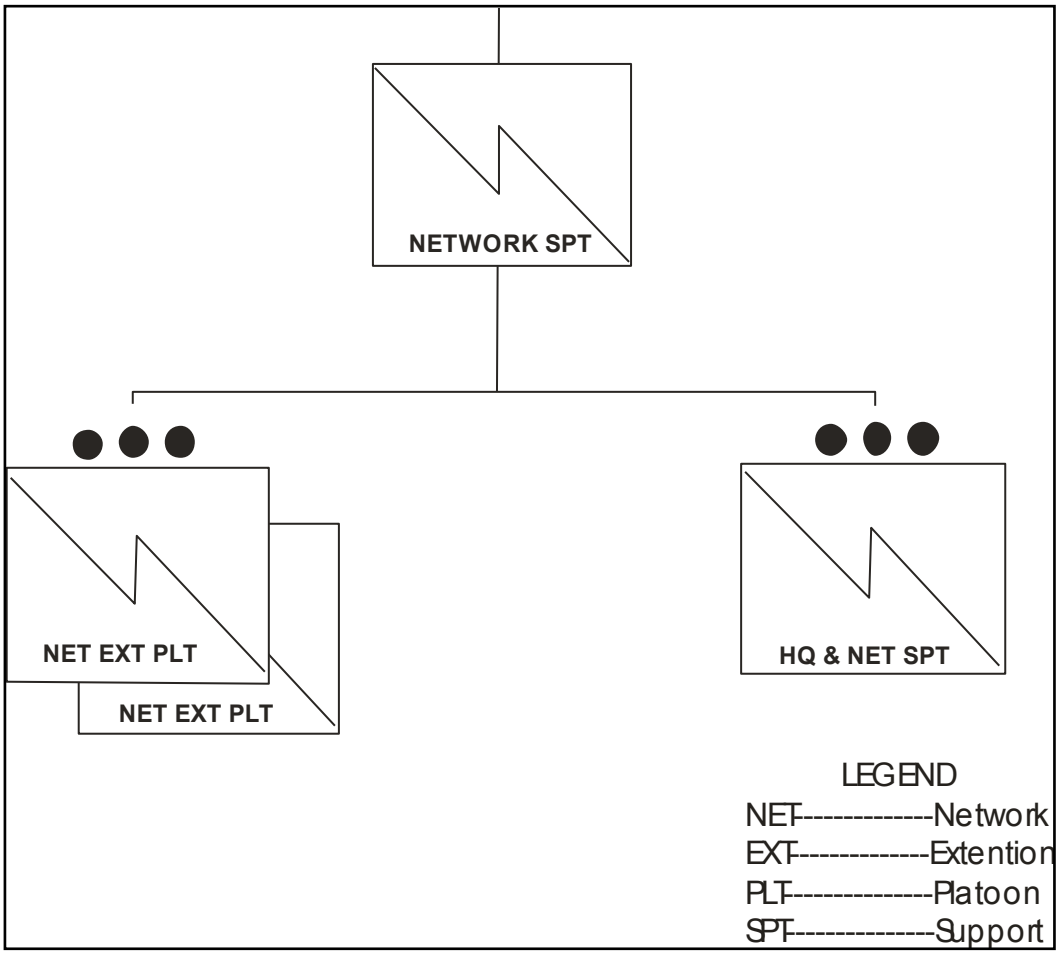

Figure 3-3. Typical BCT signal company structure

3-62. There is one CPN located at the battalion level to provide voice and data capabilities. It uses time division multiple access (TDMA) satellite transmission to gain access through the JNN or UHN to the GIG. The CPN consists of a Ku band trailer and associated transit cases to provide a wide array of services. Figure 3-4 shows battalion connectivity to the brigade using the TDMA mesh.

3-63. The CPN is located at the battalion command post (CP), and the battalion S-6 typically exercises control from this location. The equipment that is used to interface with the CPN in the CP is organic to the unit; therefore the unit sets up and operates the equipment with technical oversight from the S-6. The battalion may have an AN-TRC-190(V1) assigned, to provide a 2 Mbps traffic capability to the brigade when the mission dictates. There is one 2.4M dish Ku band satellite transportable terminal (STT) fielded to provide direct reach capabilities to higher command and or strategic enclaves using frequency division multiple access (FDMA) and TDMA

3-64. The personnel to operate the CPN are assigned to the S-6 section.

3-65. The battalion S-6 exercises control for the NETOPS assets and related operations within the battalion AOR and works closely with higher and adjacent headquarters to ensure efficient NETOPS employment and management. The S-6 section personnel are task organized and located within battalion command posts to support the commander's NETOPS requirements. See Appendix E for a diagram of a battalion to brigade and division layout.

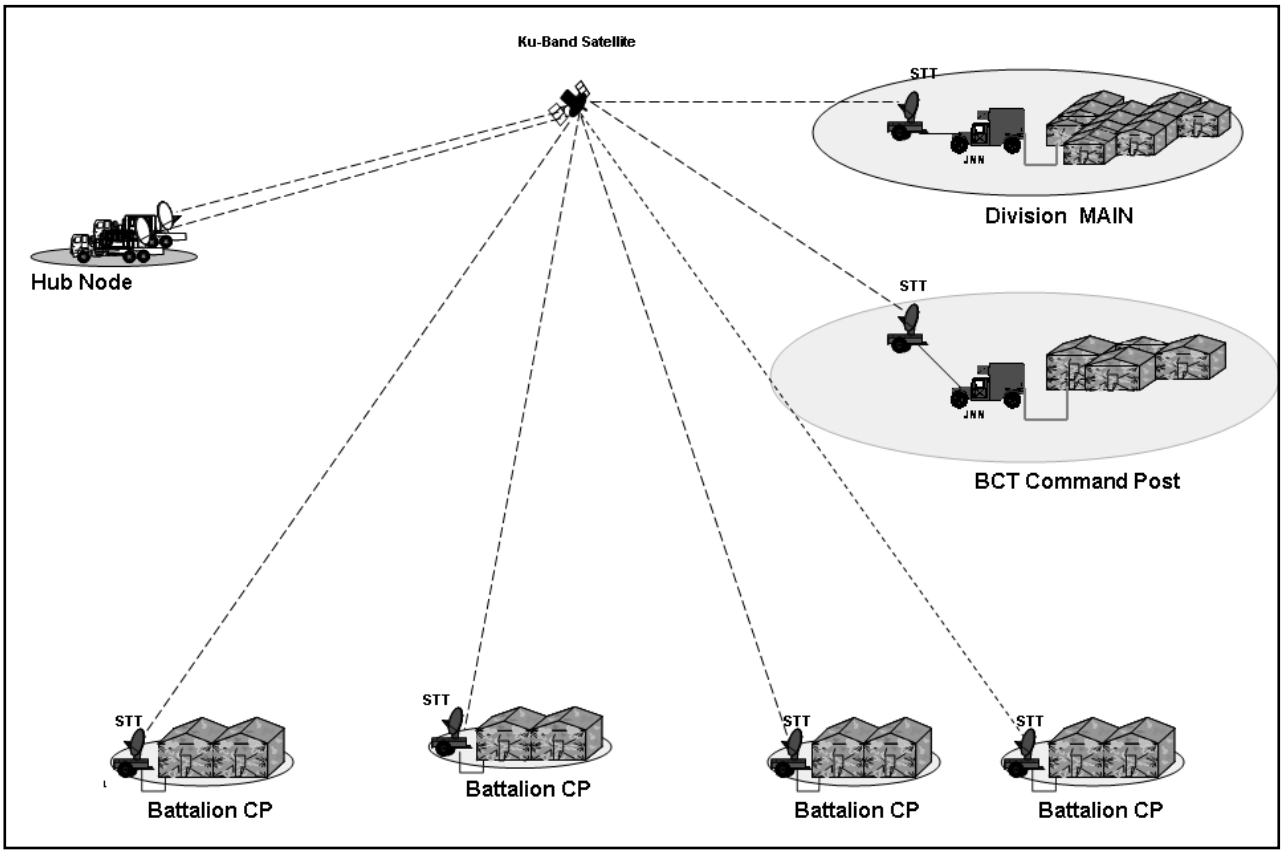

Figure 3-4. Battalion Command Post Connectivity

3-66. The S-6 in a Stryker Brigade Combat Team (SBCT) battalion is the primary planner for battalion communications operations. The S6 advises the battalion commander, staff, and the maneuver companies on all signal and communication matters. The section provides trained communications personnel to each maneuver company, and they coordinate closely with the S3 section to ensure and maintain clear lines of communication during tactical operations. The communications section is responsible for the transfer of information, the networking of automated systems, and the development of communications policies, procedures, and training for the battalion commander. For additional information on the S-6 section of a SBCT battalion see FM 3-21.21.

3-67. The battalion S6 manages the operations of communications systems received from the SBCT communications systems to support their organization as well as the battalion's own communications systems. The battalion S-6 maintains the battalion's C2 and communications systems. As a principal staff officer, the battalion S-6 interacts closely with the commander, XO, S3, and other staff officers to determine specific or unique signal requirements and develop situational understanding of the area of operation. He/she has OPCON of attached signal personnel. The battalion S6—

- Participates in the planning and operations process of the battalion.
- Coordinates closely with the brigade S6 on planning and operating the TI as it relates to the battalion.
- Understands the capabilities and operation of all communication and automation equipment in the battalion.
- Advises the battalion staff on communications matters.
- Receives and validates Enhanced Position Location Reporting System (EPLRS) VHSIC requirements and provides these to the SBCT signal officer.

- Maintains the status of communications systems operating in the battalion.
- Coordinates employment and operation of the SIV assigned for network management.
- Keeps the systems integration vehicle team apprised of battalion mission operations.
- Exercises supervisory responsibility for training and assigning the signal support system specialists in the battalion.
- Develops a concise signal annex to the battalion OPLAN or OPORD.
- Tracks COMSEC distribution within the battalion.

3-68. The infantry battalions signal officer (S-6) is the primary planner for battalion communication operations. He/she advises the battalion commander, staff, and the maneuver companies on all signal and communication matters. The duties of the battalion signal officer include—

- Plans, manages, and directs all aspects of the unit communications systems.
- Plans, supervises integration of communications with headquarters up, down, and adjacent.
- Supervises the communications activities of subordinate and attached units.
- Supervises unit maintenance of signal equipment for the unit and for subordinate units.
- Monitors status of support maintenance on unit and subordinate unit signal equipment.
- Prepares and writes the signal annex of unit orders and plans.
- Advises commander and staff on electronic counter-counter measures (ECCM) and develops reporting procedures.
- Helps the S-3 determine the location of the main, combat trains and field trains CPs.
- Ensures selected areas offer the best communications and the least interference.

3-69. The infantry battalion S-6 section is responsible for performing limited unit level repair and maintenance. It also conducts evacuation of the battalion's digital and wire communications equipment as well as maintenance of the digital system architecture that connects platoon, company and battalion to the BCT and higher networks; and on both secure and non-secure local area networks. The communications section also has the capability to provide two retrans stations for the battalion, and normally provides one Soldier to each company during operations as a communications equipment expert. For additional information on the S-6 section of an infantry battalion see FM 3-21.20.

3-70. The Field Artillery (FA) Battalion S6 is responsible for communications and automation operations, management, and security. The S6 is a coordinating staff officer and is directly accountable to the XO. For additional information on the S-6 section of a field artillery battalion see FM 3-09.21.In addition to those listed in FM 101-5, S6 duties include the following:

- Advise the commander and staff on:
    - Selection of unit position areas (PAs), from a communications standpoint.
    - Communications and automation planning, operations, priorities, security, training, and rehearsals.
    - ECCM.
    - Communications and automation requirements associated with essential fire support tasks and essential field artillery tasks, e.g., unique communications and/or automation equipment, nets, database exchange, or procedures for sensor-to shooter links or other critical communications.
- Plan, manage, and direct communications operations to include establishment of communications networks and systems and installation and maintenance of equipment.
    - Coordinate integration of battalion communications systems into those of a supported maneuver/FA unit and a FA HQ.
    - Coordinate with signal units for communications support.
    - Supervise operator and organizational maintenance of communication equipment.
    - Manage all frequency allocations and assignments.

- Manage and direct COMSEC. Direct and supervise the battalion COMSEC custodian who issues and accounts for COMSEC equipment, key lists, codes, ciphers, signal operating instructions (SOI), and authentication systems.
- Plan, manage, and direct automation systems administration, maintenance, and security.
    - Establish automation systems administration and security procedures for automation hardware and software.
    - Supervise and direct battalion local area networks configuration and usage of battalion network capabilities.
- Prepare communications estimates and write the signal paragraph (paragraph 4a) of the field artillery support plan.
- Perform communications reconnaissance and survey to assist the S3 in positioning key elements of the battalion, to include retransmission (retrans) stations.

NETOPS OPERATORS OR MANAGERS

3-71. Network managers have similar responsibilities for ESM/NM, IA/CND, and IDM/CS in many different organizations and echelons. Network managers are in units and agencies at the strategic and theater tactical military operations. At the strategic and theater tactical level, the JTF-GNO is the highest echelon of NETOPS control. A LAN manager or system administrator at a department or agency within the sustaining base is the lowest echelon. Network management positions at the operational level are at brigades, battalions, and companies supporting a theater.

3-72. Each network manager is responsible for operating, managing, and defending his portion of the network while sharing additional responsibilities with other network managers in a network. They have similar core responsibilities and perform many of the same activities, functions, and tasks. They plan, engineer, and manage networks that consist of transmission systems, circuit switches, data switches, routers, other devices, and information systems. Network management is hierarchical; therefore, network managers take direction from higher-level network managers and provide direction to lower-level network managers.

3-73. The network manager and operators uses NETOPS tools to identify potential problems and prioritize actions to be taken within the network or information system. If the network manager/operator suspects a problem is developing (when notified by alarm or person), he consults with his staff to determine root cause and correct the problem or escalates it to the responsible NOSC for resolution. Network managers must have knowledge of every aspect and the makeup of the network as well as the connectivity of the various information systems in the network. The network manager—

- Provides users with quality service of voice, data, and video networks.
- Provides a single point of control within a domain for critical NETOPS issues.
- Identifies and requests hardware and software requirements of nodes and site configuration for the network.
- Reports and escalates network and circuit outages to the appropriate service provider.
- Conforms to hardware, software, and communications architecture standards for proper NETOPS.
- Monitors overall network performance.
- Applies information systems security standards for network information, access, transmission, storage, and processing.
- Establishes network priorities.
- Focuses on network level issues.
- Records and processes information gathered from NETOPS systems that monitor the operation and security of the network, and collects and reports NETOPS statistics, e.g., bandwidth usage, error rates, and equipment failure rates for trend analysis and higher echelons.
- Identifies and diagnoses installations used in correcting network problems.

- Recommends general policy on the operation of a network based on detailed historical information.
- Establishes and monitors security by applying security standards IAW applicable regulations, standards, and TNOSC.
- Executes service desk capabilities for network operational problems and provides remote site operations support.
- Uses managed elements to enable a remote management capability.
- Depending on the unit of assignment, performs activities, functions, and tasks in the areas of network engineering, transmission management, frequency assignment, systems control, etc.

USER

3-74. The user is responsible for proper and acceptable use of his terminal devices. The user shall not change the configuration or security of his terminal device except under the written conditions established by the responsible NETOPS manager. Commanders and their staffs are the primary users of the networks provided by the signal units located throughout all military operations. Along with staff duties and responsibilities, the staff officer integrates and uses the warfighting function or other information systems to support the mission. The staff officer coordinates with the S-6 or G-6 (depending on the operational level of the unit) in all aspects of planning, implementing, integrating, operating, managing, and maintaining these information systems. The user operates—

- Warfighting function, information systems, and equipment under his/her control.
- Command and control systems and associated peripherals.
- The Standard Army Management Information System.
- Office automation.
- Radios.
- Hardware and software applications.
- Other user-owned devices.

3-75. The user is also responsible for the functional operation, troubleshooting, and maintenance IAW the user's limitations. If a system or device malfunctions, the situation should be reported to the support NOSC. The NETOPS manager or system administrator will provide connectivity and configuration advice, where needed. (For information outlining the responsibilities of the system administrator, refer to AR 25-2.)

Chapter 4
Network Operations Control Centers

This chapter identifies and describes the organizations that perform NETOPS functions to manage, control, and secure the GIG at the strategic to the theater tactical level of operations. This chapter also identifies and describes the control centers that perform NETOPS functions to manage, control, and secure tactical networks and their interfaces into the GIG. With a thorough understanding of the hierarchy of communications systems and network control, signal commanders and staff can better manage and control communications systems operation support.

GLOBAL INFORMATION GRID NETWORK OPERATIONS CONTROL CENTERS

4-1. Within the GIG, many organizations perform network and information systems management, security, and operational direction and control functions. These organizations ensure the GIG is managed through an established hierarchy of NETOPS control centers. These control centers are located at the global, theater, and tactical levels. Each center performs integrated GEM, GND, and GCM functions supporting communications system and information systems. USSTRATCOM, joint and unified commands, and Service components operate, manage, and staff these centers to control their portion of the GIG.

4-2. The GIG NETOPS control centers, at all echelons, ensure that the Soldier and all DOD components can obtain and sustain responsive, reliable, secure, and effective GIG services.

4-3. NETOPS architecture is focused on central management from higher-level echelons with overall responsibility for joint NETOPS in each theater residing under the CCDR. The CCDR relies on support from USSTRATCOM, JTF-GNO, and the numbered Army SC(T). The USSTRATCOM provides each CCDR a TNC as an additional asset, and each TNC falls under the tactical control of the CCDR. Each CCDR is required to establish a TNCC which assists them in maintaining SA and provides them with operational and tactical control of their respective system and network environment.

4-4. Each TNC provides direct support to its TNCC, ensuring the effective operation and defense of the GIG within the theater. The TNC is OPCON to JTF-GNO and offers onsite, theater support. Each TNC can issue technical directives to the A-GNOSC. The TNC develops monitors and maintains a GIG SA view for the theater. The theater GIG SA view is aggregated and segmented based on requirements provided by the TNCC as derived from the GIG common SA standards. The GIG SA view will include pertinent theater, operational, and tactical-level system and network, GND, and GCM status. Coordination with the TNCC is paramount especially with regards to reporting requirements and SA.

4-5. Successful operations of NETOPS control centers rely on compatibility, interoperability, and the integration of policies, procedures, standards, and tools. Shared USSTRATCOM, CCDR, and Service component requirements and responsibilities for successful end-to-end management of the GIG include:

- Identification of infrastructure dependencies and vulnerabilities.
- Coordination of operational response and reporting.
- End-to-end CM and review.
- Identification of network and systems purpose, criticality, interdependencies, and information flow.
- Integration of policies, operations, and tools.

GLOBAL LEVEL

4-6. Organizations with NETOPS responsibilities at the global level include: Chairman of the Joint Staff, National Military Command Center, USSTRATCOM, JTF-GNO, GNC, National Security Incident Response Center, functional combatant commands, and Service and agency headquarters.

4-7. Figure 4-1 graphically portrays the command and control relationships for GNO. CDRUSSTRATCOM is the supported commander for GNO. The other CCDRs are supporting commanders to USSTRATCOM for GNO. This relationship gives CDRUSSTRATCOM the authority to direct the CC/S/A to take action to ensure the availability and integrity of the GIG. While this relationship gives the CDRUSSTRATCOM global authority, it does not take away the CCDRs' authority over their assigned NETOPS forces. For GNO issues, USSTRATCOM will issue orders and alerts through JTF-GNO to the CCDR, Services, and agencies.

4-8. The CCDR, Services, and agencies will direct compliance with these directives within their AOR using their inherent authority over assigned forces. This construct will allow USSTRATCOM to exercise its global authority while strengthening the responsibilities of the other CCDRs. The TNCs will fall under the OPCON of JTF-GNO for GNO issues. This allows the JTF-GNO to immediately direct action by the TNCs when necessary to protect the GIG. JTF-GNO will ensure that the CCDRs are informed about all GNO issues. This OPCON relationship gives JTF-GNO the authority to issue immediate directives when necessary. The TNCs will provide direct support to the TNCCs and general support to the GNCCs in executing JTF-GNO directives.

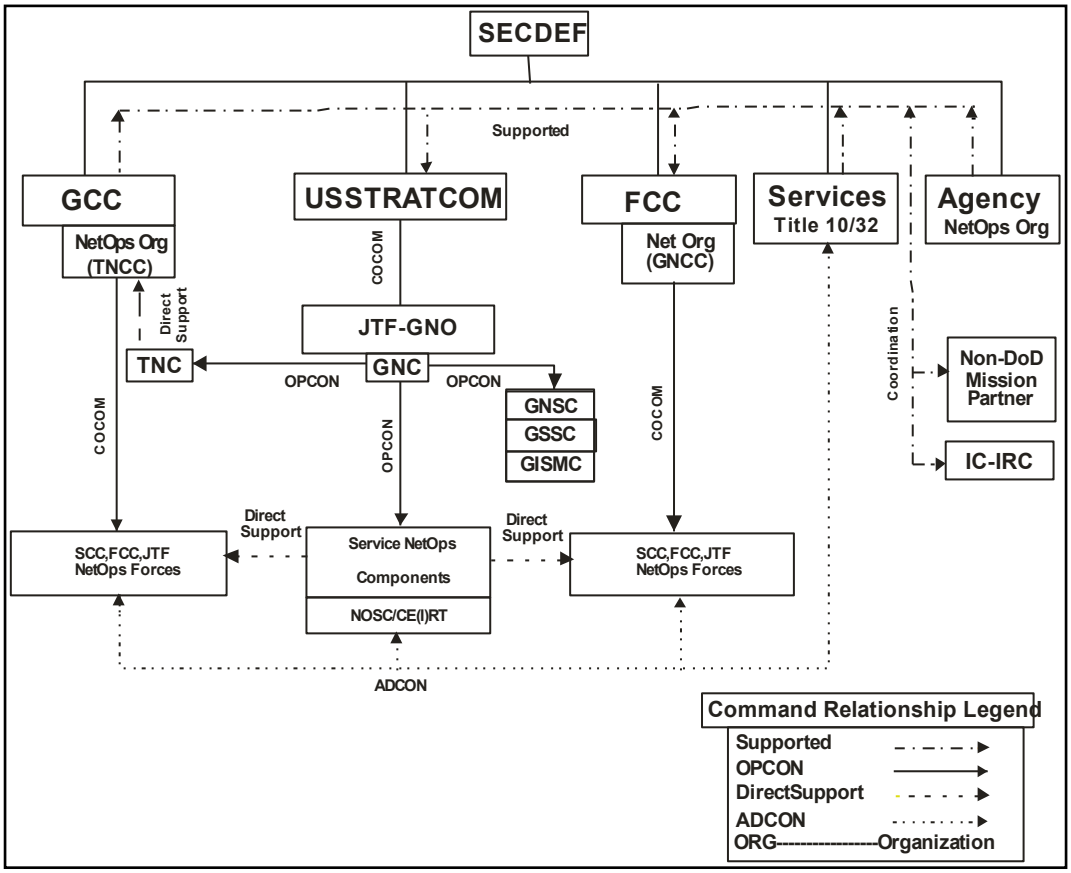

Figure 4-1. Global NETOPS command and control

4-9. JTF-GNO exercises OPCON of Service GNO units through the ASCC. For the Army, The A-GNOSC is OPCON to JTF-GNO through USARSTRAT. Defense agencies will follow the NETOPS orders

and directives issued by USSTRATCOM and JTF-GNO. Service and Agency Systems Management Centers and Central Design Authorities are in general support of JTF-GNO, ensuring that the systems they operate and provide as parts of the GIG are compliant with JTF-GNO guidance.

COMMANDER, JOINT TASK FORCE-GLOBAL NETWORK OPERATIONS

4-10. The CJTF-GNO will lead and direct continuous GEM, GND, and GCM throughout the GIG. To ensure global decision superiority, they will maintain near real-time SA, end-to-end management, and dynamic GIG defense.

4-11. The CJTF-GNO will also exercise OPCON of the GIG for global network operations issues. global network operations issues are those where action or inaction potentially affects multiple CCDR, Services, and agencies. Under the authority of CDRUSSTRATCOM, JTF-GNO will issue the orders and directives necessary to maintain the assured service of the GIG. This ensures that the President, SECDEF, CCDRs, and Services and agencies can accomplish their missions. The CCDR, Services, and agencies will execute JTF-GNO's directives within their respective areas and report compliance. To achieve this mission, the CDRUSSTRATCOM has assigned these tasks to the commander of JTF-GNO. The commander of JTF-GNO has the following tasks:

- Direct GIG NETOPS to ensure confidentiality, integrity, availability and efficiency of the GIG infrastructure and information services.
- Establish and maintain SA of the GIG and report readiness and defensive posture to HQ USSTRATCOM, as required.
- Coordinate with HQ USSTRATCOM staff and subordinate organizations, as required, during the development, acquisition, implementation, promulgation and operation of NETOPS joint tactics techniques procedures and tools intended for monitoring performance, threats, policy compliance and controlling network access.
- Assist in identifying, establishing and maintaining GIG NETOPS characteristics, capabilities, standards and requisite measures of effectiveness for infrastructure and information services.
- Direct and oversee NETOPS and defense capabilities. Synchronize network defense capabilities with the Joint Functional Component Command Network Warfare (JFCC-NW), the joint IO warfare command and other USSTRATCOM components, as necessary. Assume OPCON or tactical control (TACON), where applicable, of NETOPS/CND forces and capabilities for day-to-day and crisis response actions.
- In collaboration with the joint IO warfare command and ICW JFCC-NW ensure that computer NETOPS (computer network attack, CND and CND response action) are synchronized for crisis and deliberate planning. These activities support USSTRATCOM JFCCs and other CCDRs' mission objectives and courses of action; including integration with supporting operational and tactical level plans, as directed by CDRUSSTRATCOM.
- Develop course of action (COA) recommendations for NETOPS, including CND and CND response action, in support of USSTRATCOM and national strategic objectives. Support the JFCCs for the integration of NETOPS into USSTRATCOM mission areas. Provide an embedded capability in the Global Operations Center to support JFCC global strike and integration mission of operational level integration of USSTRATCOM missions and maintaining SA for the commander.
- Establish procedures to conduct CND response action IAW DOD policy and coordinate with JFCC-NW for Tier 1 CND RAs. CDRUSSTRATCOM retains the execution authority and responsibility for those procedures.
- Oversee procedures to establish and provide measures of effectiveness and damage assessment as a part of network defense operations.
- Provide support for USSTRATCOM and other geographic and functional CCDRs' exercises, wargames and experimentation requirements involving NETOPS. Integrate and synchronize efforts with USSTRATCOM Training and Exercise Division.

- Provide network defense priority intelligence requirements, requests for intelligence, intelligence production requirements and intelligence collection requirements with USSTRATCOM J-2 for tasking, deconfliction and accomplishment.
- Perform all-source analysis of threats to the GIG, including threat analysis of foreign malicious activity, ICW USSTRATCOM J-2, JFCC ISR, and JFCC-NW. Provide assessments and recommendations to CDRUSSTRATCOM and other CCDRs for changes dictated in network threat warning and INFOCON procedures.
- Establish a relationship with mission area experts in the applicable GCC Standing Joint Force Headquarters to provide operational support for NETOPS with emphasis on CND capabilities. This relationship will include the training and periodic qualification of NETOPS support in Standing Joint Force Headquarters, as required.
- Support USSTRATCOM development and execution of NETOPS assessments, research and development efforts and advocacy of capability needs for the Joint Capabilities Integration Development System process.
- Support USSTRATCOM and JFCC's led efforts to create and maintain strategic-level operations plans. Support development and coordination of NETOPS and command, control, communications and computers portions of operations plans, concept plans, functional plans, and supplemental plans as directed by headquarters. Support other combatant commands with NETOPS and command, control, communications and computers operational planning and execution, as directed by headquarters.
- Develop and coordinate NETOPS CONOPS.

COMMANDER OF THE GLOBAL NETWORK OPERATIONS CENTER

4-12. The CJTF-GNO has established the GNC as a subordinate command responsible for executing the daily operation and defense of the GIG. The GNC directs, manages, controls, monitors, and reports on essential elements and applications of the GIG in order to ensure its availability to support the needs of the President, SECDEF, CCDRs, Services, agencies, and business and intelligence domains. The GNC coordinates through technical channels the overall management, control, and guidance for GIG NETOPS and oversees a collaborative coordination process involving all CC/S/A. The GNC has the following responsibilities:

- Direct the operation and defense of the GIG.
- Collaborate with the NETOPS community to ensure effective operation and defense of the GIG.
- Advise CDR, JTF-GNO and CDRUSSTRATCOM on matters regarding the allocation and adjudication of GIG resources.
- Advise CDR, JTF-GNO and CDRUSSTRATCOM of any matters impacting the GIG’s integrity and/or NETOPS issues affecting DOD missions.
- ICW CC/S/A, establish and maintain the technical and operational standards by which the GIG SA will be generated across the GIG.
- Provide a consolidated global SA view to the GCCs/TNCCs and other NETOPs components.
- Ensure close coordination between the global satellite communications support center (GSSC) and the Joint Space Operations Center to ensure anomaly/incident management can support SA.
- Perform global incident/intrusion monitoring and detection, strategic vulnerability
- Analysis, media analysis, and responses to GND-related activity.
- Direct COA and coordinate the CND incident RAs across DOD to defend networks under attack.
- Determine COA and direct restoral of GIG capabilities and services when required.
- Maintain GIG SA in support of each CCDRs current and near term operations as well as deliberate plans.
- Maintain visibility, to include security monitoring of the GIG, through an integrated GIG SA view. This is achieved through the integration of the TNC and Service/agency collected and

shared GIG SA data. This shared SA view includes wireless, terrestrial, SATCOM systems, enterprise services, and limited logical and physical infrastructure views of the networks.

- Identify, localize, and resolve GIG security anomalies that affect the GIG's ability to support senior military leadership at the national level, Joint Staff, and supported CCDR.
- Coordinate GND support to the CCDR.
- Coordinate with and receive support from the DOD law enforcement and counterintelligence center.

4-13. The GNC establishes procedures facilitating the ability of geographic commanders who share common GIG assets to:

- Consider the impact of one's own actions or inactions on adjacent commanders and related business and intelligence communities.
- Provide access to timely information among adjacent commanders regarding others' intentions and actions, as well as those of non-military agencies or the enemy, which may influence adjacent activity.
- Support adjacent commanders, as required, by establishing a common aim and monitoring the unfolding situation.
- Coordinate the support provided and received.

COMMANDER OF THE GLOBAL NETWORK OPERATIONS SUPPORT CENTER

4-14. The CJTF-GNO will create a subordinate command to provide the day-to-day technical operation, control, and management of the portions of the GIG that support global operations but are not assigned to a CCDR. The GNSC will conduct GIG backbone NETOPS, STEP mission support, provisioning of provided services, network engineering, circuit implementation and inter-theater connectivity among the US Army Northern Command; US Army, Pacific Command; US Army, European Command; USARSO; and US Central Command AORs. The GNSC will provide general support to the GCCs and TNCs. The GNSC will provide direct support to the functional CCDRs.

4-15. The GNSC will provide full-time (24 hours a day, seven days a week), near real-time, correlated visibility, monitoring, coordination, control, and management support of the global backbone portions of the GIG. The commander of the GNSC will develop, monitor, and maintain a GIG SA view for the global backbone. To carry out its mission, the GNSC—

- Operates and maintains GIG backbone services within the CONUS boundaries to include services originating within CONUS to OCONUS locations.
- Collaborates with the CC/S/As NETOPS centers to ensure effective operation and defense of the GIG.
- Advises the GNC on issues relative to the allocation and performance of GIG backbone resources.
- Advises the GNC of issues impacting the integrity of the GIG and/or NETOPS issues affecting DOD missions.
- Works collaboratively with the GNC and the CC/S/As to establish and maintain the technical and operational standards by which information sharing and status reporting will be implemented to fully enable NETOPS.
- Ensures compliance with JTF-GNO issued directives and guidance within their respective areas of responsibility.
- Provides SA information for backbone services within their boundaries of the GIG.
- Monitors and collects performance and trending data for those GIG resources deemed important by JTF-GNO.
- Provides system and network status (fault and performance) information for their portion of the global SA view.

- Assists in the correlation and analysis to determine the technical and operational mission impacts caused by degradations, outages, and GND events.
- Performs global, theater, and non-global incident/intrusion monitoring and detection, strategic vulnerability analysis, media analysis, and coordinates responses to GND-related activities. Directs the execution of CND incident RAs within their respective areas of responsibility to defend networks under attack.
- Determines COAs and directs the restoral of capabilities and services as required.
- Maintains SA in support of each functional component commander's current, near term, and deliberate planning operations, as required.
- Maintains security monitoring through an integrated GIG sensor grid.
- Coordinates with and receive support from the law enforcement/counter-intelligence community.

FUNCTIONAL COMBATANT COMMANDS (UNITED STATES STRATEGIC COMMAND, UNITED STATES SPECIAL OPERATIONS COMMAND, UNITED STATES JOINT FORCES COMMAND, AND UNITED STATES TRANSPORTATION COMMAND)

4-16. Functional CCDRs have a global mission, often providing support to the GCCs, and have a global requirement for NETOPS support. Some functional CCDRs operate their own function-specific global network, Joint National Training Capability, Global Transportation Network, and Ballistic Missile Defense. The functional CCDRs will receive direct support from the GNSC and general support from USSTRATCOM, JTF-GNO, and all TNCs. Functional CCDRs will exercise OPCON over their portions of the GIG through their GNCC. The GNCC will coordinate the functional CCDR's NETOPS requirements with the GNSC and the TNCCs.

GLOBAL NETOPS CONTROL CENTER

4-17. The primary mission of a GNCC is to advise the functional CCDR and ensure the portion of the GIG resources supporting the commander's assigned missions and operations are optimized. To be effective, each GNCC must remain cognizant of all current, future, or contemplated operations in which their portion of the GIG will play a role.

4-18. The GNCCs monitor the CCDR's GIG assets, determine operational impact of major degradations and outages, and coordinate responses to degradations and outages that affect joint operations. Each GNCC will coordinate with the GNC and support any TNC mission or operational impacts that are associated with system and network anomalies or resource limitations. Additionally, the GNCC has direct liaison authorization with the TNCCs. This authorization gives the GNCCs and TNCCs the ability to directly coordinate scheduled changes in the GIG or troubleshoot outages.

SERVICES AND AGENCIES

4-19. The Services and defense agencies provide, operate, and maintain the vast majority of the equipment, personnel, and other resources that make up the GIG. Execution of these functions requires the Services and agencies to be actively engaged in NETOPS of the GIG. To execute these functions, the Services and most agencies have established NOSCs, which maintain SA of their portions of the GIG. In this manual, these organizations are called Service and agency global NOSCs.

4-20. These Service GNOSCs and agency GNOSCs serve as a central point of contact for matters concerning the resources they provide to the GIG. JTF-GNO will exercise OPCON of the Service GNOSCs. DOD agencies will align their agency GNOSCs to provide USSTRATCOM visibility and insight of their GIG status and will follow the orders and directives issued by JTF-GNO. Services and agencies will maintain a global perspective of their GIG assets and provide service specific support to the global network operations mission. This global SA is necessary for the Service and agency to properly provide the equipment, personnel, and other resources they contribute to the GIG. The Army executes its Service GNOSC responsibilities via the A-GNOSC and the ACERT (also known as the A2TOC).

ARMY GLOBAL NETWORK OPERATIONS AND SECURITY CENTER

4-21. The A-GNOSC is the Army's execution arm for Operations, Management and Defense of the LWN. The A-GNOSC executes this responsibility using the NETOPS construct. The A-GNOSC uses the NETOPS essential tasks of ESM/NM, IA/CND and IDM/CS to execute its responsibilities in order to achieve LWN availability, LWN information protection and delivery. The A-GNOSC synchronizes, coordinates and directs all Army LWN IT/information management service management, through the TNOSC in each ASCC; the ACOMSs, the direct reporting units, and the PEOs. The A-GNOSC is responsible for acquiring and providing NETOPS SA to the Army decision makers at all echelons.

Service Responsibilities

4-22. As the first step in achieving GNO, the SECDEF has approved the transfer of OPCON of the A-GNOSC to CDRUSSTRATCOM through the designated Service component (ARSTRAT) headquarters for CND per Headquarters Department of the Army Computer Network Operations Standing Execute Order. CDRUSSTRATCOM will further delegate OPCON of the A-GNOSC to JTF-GNO. The A-GNOSC serves as a part of the Service component to JTF-GNO. The A-GNOSC mission is to provide the Army-specific NETOPS reporting and SA for the Army's portion of the GIG. The A-GNOSC provides worldwide operational and technical support to the Army's portion of the GIG across the strategic, operational, and tactical levels, leveraging collaboration of the established TNOSC. The Army NOSC is integrated with the 1st IO CMD ACERT to create a consolidated NETOPS center called A2TOC. This alignment of organizations provides a critical synergism of effectiveness and efficiency to receive, distribute, and analyze information in order to integrate, synchronize, and coordinate Army NETOPS.

Note. To enhance the A-GNOSC support to the CDRUSSTRATCOM in CND, Appendix F will provide the CND view of the LandWarNet information assurance architecture (LIAA).

THEATER LEVEL

4-23. The theater portion of the GIG, from the operational perspective, is comprised of that portion of the GIG operated by a Geographic Unified Command, its sub-unified and component commands, its joint and single-service task forces, and installations and activities within the AOR. From a technical perspective, it is a subset of GIG assets, resources, and services.

4-24. Figure 4-2 depicts the command and control relationships for theater NETOPS. The theater CCDR exercises OPCON of all assigned NETOPS forces and their portion of the GIG. The USSTRATCOM TNC is under the tactical control of the theater CCDR for theater NETOPS issues. The CCDR's TNCC is responsible for the operation of their portion of the GIG and issues directives to the TNC and component NETOPS organizations to ensure that the GIG supports the theater mission. USSTRATCOM and JTF-GNO are in support of the theater CCDR and ensure that the GIG is capable of supporting the theater CCDR's requirements.

4-25. When there are conflicts or resource contention between CCDRs' requirements, JTF-GNO will deconflict resource requirements. Competing resource requirements that cannot be resolved will be forwarded through CDRUSSTRATCOM to the CJCS for adjudication. The Service and agencies may establish theater-level NOSCs or provide 24 hours a day, seven days a week theater level SA to support the requirements of the CCDRs and their Service components. Either the global or theater NOSC will provide theater GIG visibility to the TNC and other DOD component NOSCs as required. This Service or agency NOSC will also serve as a central point of contact for operational matters and emergency provisioning for a supported CCDR. This will enable improved GIG SA at all levels of the command structure and facilitate end-to-end GIG management.

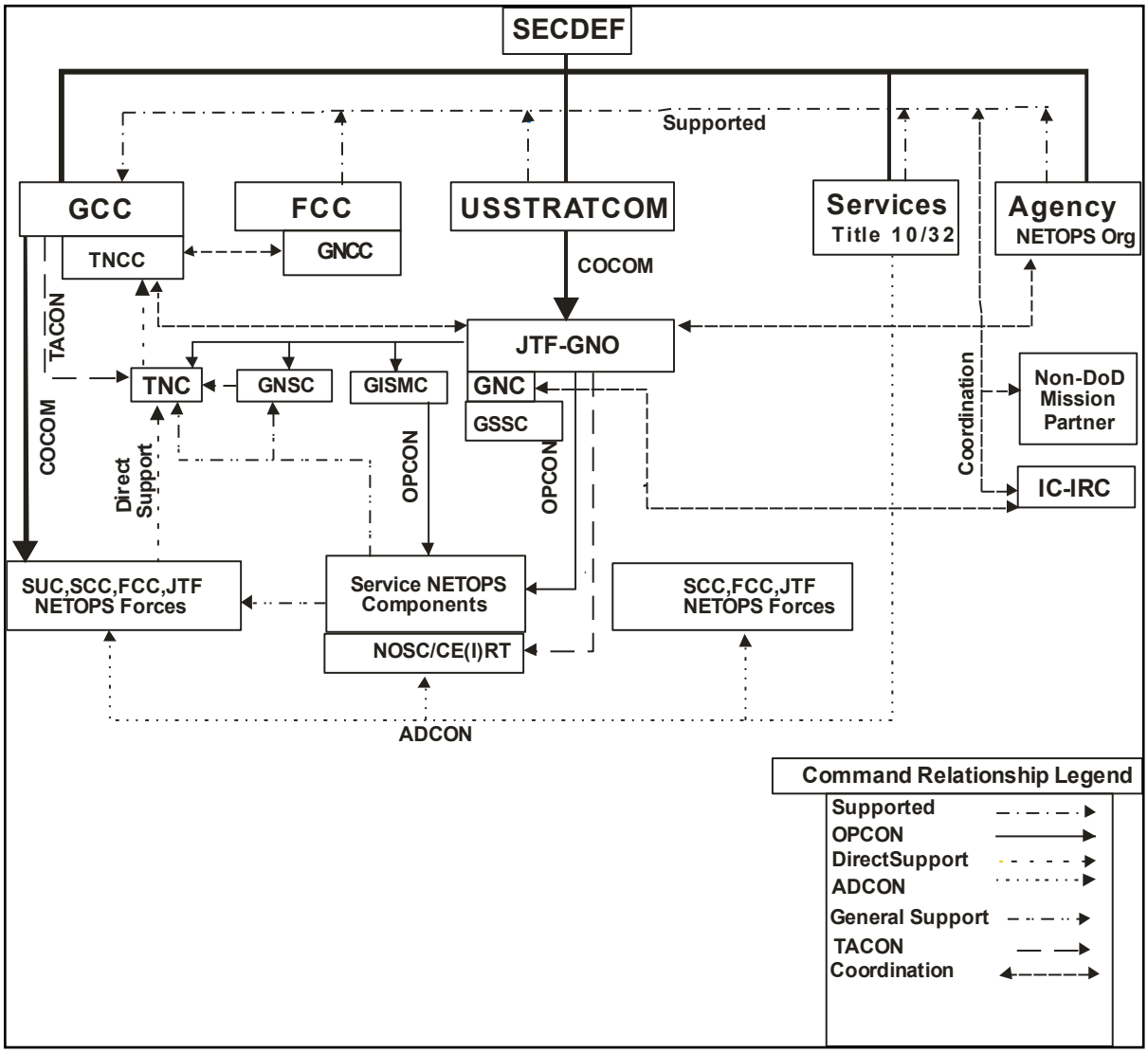

Figure 4-2. Theater NETOPS command and control

GEOGRAPHIC COMBATANT COMMANDS (UNITED STATES CENTRAL COMMAND, UNITED STATES EUROPEAN COMMAND, UNITED STATES PACIFIC COMMAND, UNITED STATES NORTHERN COMMAND, UNITED STATES SOUTHERN COMMAND)

4-26. The GCC exercises OPCON over the GIG and component NETOPS forces, and exercises tactical control over the TNC for theater NETOPS matters. To accomplish this, all GCCs will establish a TNCC, through which they will maintain SA and exercise OPCON and tactical control of their apportioned, allocated, or assigned system and network environment. The CCDR's main operations responsibility at the theater level is to direct, establish, and control the systems and networks used to conduct command and control of the CCDR's mission.

THEATER NETWORK OPERATIONS CONTROL CENTER

4-27. The primary mission of the TNCC is to lead, prioritize, and direct GIG resources to ensure they are optimized to support the GCC's assigned missions and operations. The TNCC is also required to advise the

CCDR of the ability of the GIG to support current and future operations. In performing its mission, the TNCC exercises OPCON over all theater systems and networks operated by forces assigned to the CCDR. The TNCC also exercises tactical control over the TNC for theater NETOPS issues. The specific roles of the TNCC include monitoring of the GIG, determining operational impact of major degradations and outages, coordinating responses to degradations and outages that affect joint operations, and coordinating GIG actions in support of changing operational priorities. The TNCC also responds to JTF-GNO direction when required to correct or mitigate a GNO issue.

4-28. The TNCC, in advising the CCDR of the GIG's ability to support assigned missions and operations, must remain cognizant of all current, future, or contemplated operations involving the GIG. This requires continual contact and coordination with the CCDR's Joint Operations Center. Serving as an operational extension to the CCDR's command center, the TNCC provides GIG SA and operational impact assessments to the commander and the Joint Operations Center.

4-29. The TNCC will use the GIG SA view provided by their TNC, component NETOPS organizations, and theater JNCCs to maintain SA over the portion of the GIG necessary for the success of their CCDR's assigned missions. Although the NETOPS SA software application will be a part of an enterprise-wide software toolset, the input data requirements and output products (picture or view reports, etc.) will be user customizable, based on built-in options, to meet the needs of each CCDR.

4-30. The TNCC is responsible for coordinating the definition and development of the content and scope of the GIG SA information view for the theater based on DOD parameters to assure complete integration. This will be based on the commander's guidance and requirements submitted by subordinate commands. The specifications will be submitted to the TNC, which is responsible for producing and disseminating the GIG SA view. Some level of minimum SA view shall be defined to ensure that all NETOPS facilities provide a consistent set of information and to make it easier to integrate and roll-up SA views generated by different theaters or organizations.

4-31. The TNCCs will direct and prioritize required operational actions through their supporting TNC and assigned NETOPS forces. System and network management activities, in response to NETOPS decisions made by the TNCC, are accomplished through the CCDR's tactical control authority over the TNC and through OPCON over forces assigned to the CCDR. In order to carry out it's mission, the TNCC will:

- Establish uniform 24 hours a day, seven days a week visibility into the status of the GIG SA view to/from the TNC and assigned NETOPS organizations.
- Collaborate with the NETOPS community of interest to ensure effective operation and defense of the GIG.
- Establish and retain visibility of system and network outages and customer service shortfalls. Receive, consolidate, and analyze all available reports from the components, agencies, JTFs, and deployed units.
- Direct reporting of NETOPS events, conduct analysis of the impact of such events on the operational mission, develop alternate COAs, and advise the commander and other senior decision makers on the status of GIG degradations, outages, GND events, and areas requiring improvement.
- Prioritize the installation and restoration of system and network services for the TNC and subordinate organizations in the form of a critical customer (i.e., decision-maker) listing.
- Direct, coordinate, and integrate response actions to computer network attacks and significant intrusions affecting the CCDR's portion of the GIG.
- Direct the theater's response to JTF-GNO directives for correcting or mitigating GNO issues.
- Coordinate with JTF-GNO to deconflict the CCDR's theater NETOPS priorities with the global network operations priorities of JTF-GNO and USSTRATCOM.
- Deconflict issues between the TNC and TNOSC/A-GNOSC.

THEATER NETWORK OPERATIONS CENTER

4-32. The TNCs OPCON to the JTF-GNO provide full-time (24 hours a day, seven days a week), near real-time, correlated visibility, monitoring, coordination, control, and management support of the CCDR, Service, and agency portions of the GIG. For example, the TNC provides the view of the GIG within a CCDR's AOR. This type of capability will include reciprocal, shareable "look-up" and "look-down" near real-time correlated views of component, sub-unified, and JTF elements of the GIG.

4-33. The commander of each TNC will develop, monitor, and maintain a GIG SA view for the theater. The theater GIG SA view will be aggregated and segmented based on requirements provided by the TNCC or GNCC. It will include pertinent theater, operational, and tactical-level system and network GND and GCM status. To carry out its mission, the TNC will—

- Operate and maintain the backbone services of the GIG assets located in their theater.
- Collaborate with the NETOPS community of interest to ensure effective operation and defense of the GIG.
- Issue technical directives to STNOSCs and agency TNOSCs to ensure compliance with TNCC and JTF-GNO direction.
- Receive SA information in order to monitor all theater service or Service component and agency systems and networks designated as mission critical.
- Support the CCDR, Services, and agencies by creating and disseminating the NETOPS SA views for the theater Service or Service component and agency. This is accomplished by integrating NETOPS event and status information received from those elements within the TNC AOR that have NETOPS reporting requirements. This shared SA view includes wireless, terrestrial, space based systems, and enterprise services.
- Coordinate with the TNCC regarding reporting requirements (input data) and view specifications for NETOPS SA.
- Continuously monitor and collect performance data for those information resources deemed important by the CCDR's TNCC or GNCC.
- Provide system and network status (fault and performance) information as part of the SA view.
- Provide the TNCC or GNCC with information security products and services to include: the monitoring and reporting of intrusions, physical threats and analysis, correlation of intrusion incidents with components, sub-unified commands, and JTFs.
- Assist in determining the technical and operational mission impacts caused by degradations, outages, and GND events.
- Perform incident and intrusion monitoring and detection, strategic vulnerability analysis, computer forensics, and responses to GND-related activity. Direct COAs and coordinate the GND incident response actions across DOD to defend networks under attack.
- Determine COAs and direct restoration of capabilities and services when required.
- Maintain SA in support of each CCDR's current and near term operations as well as deliberate plans.
- Maintain security monitoring through an integrated GIG SA view. This is achieved through integration of TNC and Service or agency collected and shared GIG SA data. This shared SA view includes wireless, terrestrial, and space-based systems and enterprise services.
- Identify and resolve computer security anomalies that affect the GIG assets located in their theater.
- Coordinate theater GND support as directed by the TNCC.
- Coordinate with and receive support from law enforcement and counterintelligence center.
- Manage theater radio frequency interference resolution, satellite anomaly resolution, and SATCOM systems.

SERVICE AND AGENCY THEATER NETWORK OPERATIONS AND SECURITY CENTERS

4-34. Service components supporting a geographical combatant command may establish TNOSCs based on the size and topology of their NETOPS responsibilities in order to provide and manage systems and network services. The TNOSC will serve as a single point of contact for their theater elements for systems and network services; ESM/NM, IA/CND, and IDM/CS capabilities; and operational reporting. The TNOSC provides GIG SA information to the TNC and the TNCC. In the absence of a TNOSC, the A-GNOSC will perform the function of the TNOSC. To facilitate end-to-end management and maintain the accuracy of the GIG SA view, each TNOSC will—

- Sub-exercise routine, day-to-day management, control, and defense of system and network services provided as part of the GIG.
- Collaborate with the NETOPS community of interest to ensure effective operation and defense of the GIG.
- Comply with GIG SA (visibility and status) reporting requirements for their portion of the GIG as determined by the CCDR.
- Provide GIG SA information specifically from the TNC points of presence to the component's deployed forces.
- Provide the TNCC or GNCC and TNC current (near real-time) SA of systems and networks under their control and within their portion of the GIG for retrieval and use by other NETOPS centers.
- Assist the TNC and the TNCC or GNCC in tracking the status of NETOPS events and determining the technical and operational mission impacts caused by NETOPS events.
- Respond to a variety of threats using a range of response measures to preclude, detect, and counter any threat.
- Exercise tactical control over the system and network resources of their assigned NOSCs, divisions, and brigades and systems administrators.

ARMY FORCES NETWORK OPERATIONS AND SECURITY CENTER

4-35. The ARFOR NOSC is provided by the SC(T)'s TNOSC. The ARFOR G-6, as a staff officer, should establish an Army NETOPS Control Center.

4-36. The Army NETOPS Control Center provides the commander's intent and direction to the TNOSC that is responsible to operate, manage, and defend the theater's portion of the LWN and GIG. The TNOSC executes the command's intent and direction for the LWN. The SC(T) or its deployed element is OPCON to the ARFOR. Thus the TNOSC or its deployed element is OPCON to the ARFOR.

THEATER NETWORK OPERATIONS AND SECURITY CENTER

4-37. The TNOSC operates, manages, and defends LWN in order to deliver seamless communications system information management capabilities in support of all in-theater Army entities in its AOR. The TNOSC executes its NETOPS responsibilities ICW the numbered Army G-6. The responsibilities of the TNOSC include the oversight of both fixed theater infrastructure as well as tactical Army units within the theater AOR. Figure 4-3 represents the TNOSC structure.

UNIFIED COMMANDS

4-38. CCDRs may organize a sub-unified command and assign tailored forces from among the four Service components and special operations forces to the sub-unified commander. The CCDR assigns the sub-unified commander OPCON of designated forces.

4-39. Sub-unified commands may establish sub-unified NETOPS control centers with responsibilities and relationships similar to a Service TNOSC. The sub-unified command's NOSC will serve as a single point of contact for their subordinate elements for systems, network services, and reporting.

SUB-UNIFIED NETOPS CONTROL CENTER

4-40. Sub-unified NETOPS control centers will provide GIG visibility and status information to the geographical combatant command's TNCC and TNC to facilitate end-to-end management and maintain accuracy of the NETOPS.

JOINT NETOPS CONTROL CENTER

4-41. The JNCC manages the tactical communications of the joint force, serving as the NOSC for the deployed portion of the GIG supporting a JTF. It exercises staff supervision over the communications system signal company belonging to deployed components and subordinate commands. The JNCC provides the appropriate TNCC with:

- GIG SA information (directly to TNCC and TNC).
- Mission impact assessments of system and network events.
- GIG requirements beyond the JTF's current assets or authority.

THEATER NETWORK OPERATIONS AND SECURITY CENTER DEPLOYMENT SUPPORT DIVISION

4-42. In conjunction with the modular restructuring of the Army, the SC(T) is undergoing revision in order to support emerging requirements of the new modular force. One revision is the addition of a new deployment support division within the TNOSC. The deployment support division has primary responsibility for all NETOPS support to deployed forces. It is comprised of two branches: the tactical network team (TNT) and the tactical integration cell (TIC). Refer to Figure 4-3 for an illustration.

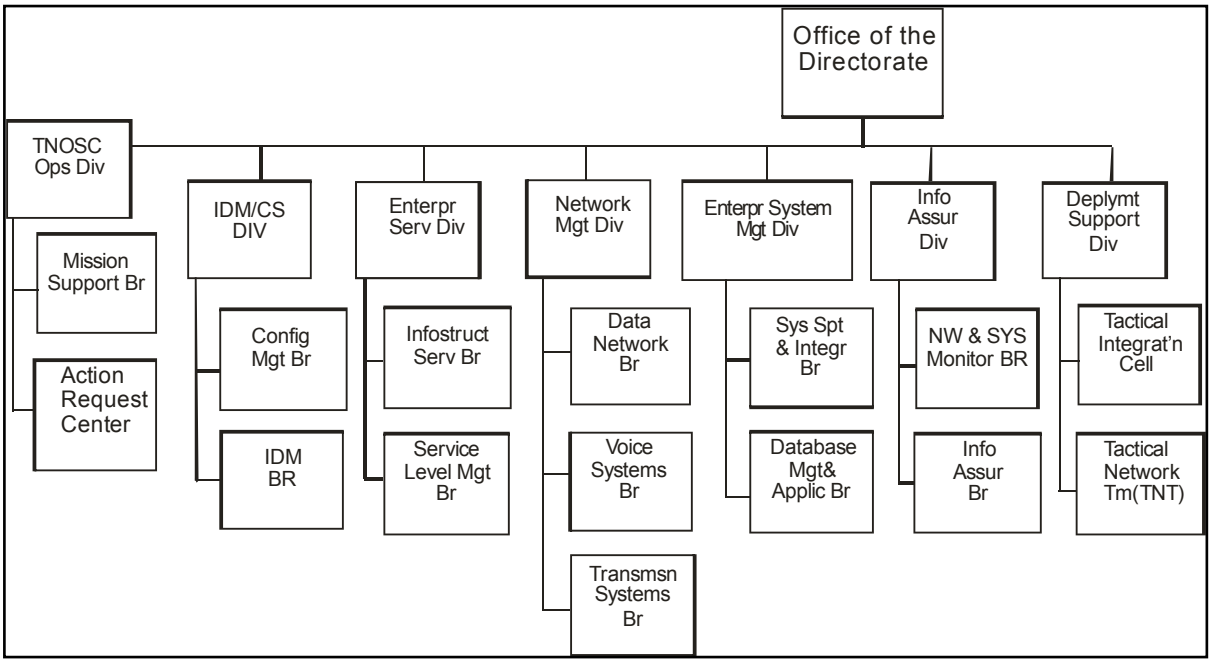

Figure 4-3. TNOSC structure

Tactical Network Team

4-43. The TNT is an authoritative NETOPS cell for a joint or Army component command. It is a fully deployable (but based on mission, enemy, terrain and weather, troops and support available-time available, it is not necessarily fully or always deployed) NETOPS entity that can provide a complement of NETOPS capabilities to a deployed headquarters. For example, the TNT could deploy to implement or augment the ARFOR NOSC supporting the JFLCC.

Tactical Integration Cell

4-44. The TIC is a body of tactical network personnel within the deployment support division of the TNOSC that is dedicated to the integration and support of tactical units. This would include oversight and management of tactical numbered Army NETOPS support services, such as the network service center regional and tactical NETOPS systems. It also includes the formation of temporary tactical liaison team (TLT), which is dedicated to support a specific tactical unit.

4-45. Other divisions under the TNOSC structure include a TNOSC Operations Division, IDM/CS Division, Enterprise Services Division, Network Management Division, Enterprise Systems Division, and the Information Assurance Division. Each division is structured with several branches reporting to the division which reports to the directorate.

TNOSC Operations Division

4-46. The TNOSC Operations Division is the analog of the S-3 in a regular battalion. It has oversight of the day-to-day operations of all divisions, focusing on larger systemic problems that require directed focus or resolution. The division consist of the following branches:

- **Mission Support Branch**. This branch provides all the administrative and logistic support for the TNOSC. Included here are the budget, personnel, and training activities. Contracting Officer's Representative duties and oversight of other contracts (for which the TNOSC is not the Contracting Officer's Representative) that affect the TNOSC. Responsible for procurements, Unfunded Requirements, Program Objective Memorandum submissions, IMPAC card, military interdepartmental purchase request tracking and coordination with resource managers. This branch operates 8 hours a day, 5 days a week.
- **Action Request Center**. This branch operates 24 hours a day, seven days a week to provide SA of all NETOPS activities that the TNOSC controls or interacts with. The staffing for the watch officers is in the action request center. This branch does all reporting to higher and lateral agencies. It provides overall direction of troubleshooting and reporting of subordinate units. This branch operates 24 hours a day, seven days a week.

Information Dissemination Management Division

4-47. The IDM Division provides the CM for the theater operations. It also determines customer info source/sink and provides immediate feedback of the accuracy of the CM documents and products providing the best feedback loop. The division consist of the following branches:

- **Configuration Management Branch**. This branch runs the theater level NETOPS CM program. It chairs the theater NETOPS CCB. It maintains the CM database and network level drawings. This branch manages the program for the theater and monitors and measures the effectiveness of subordinate CM programs. Coordinates with the theater Army G-6 and signal command theater program managers to insure projects are included in the CM process. This branch works 8 hours a day, 5 days a week.
- **IDM Branch**. This branch manages the theater IDM program, establishing the architecture and overseeing the IDM efforts of subordinate NOSCs. Coordinates IDM with other divisions and teams. Provides expertise to incorporate IDM into communications planning, optimizes IDM infrastructure resources, analyzes and documents IDM requirements and implements IDM enabling technology to include CS. This branch works 8 hours a day, 5 days a week.

ENTERPRISE SERVICES DIVISION

4-48. The Enterprise Services Division operates the applications (as opposed to the networks) that provide the enterprise network services and enable the management of the enterprise "down to the desktop". This division also tracks and monitors operation of the area processing centers (APC) in theater. The division consist of the following branches:

- **Infostructure Services Branch**. This branch manages the services that the networks provide to enable the customers to utilize the enterprise. These services would include DNS, Remote Authentication Dial-In User Server (RADIUS), and remote access services (VPN program). It includes management of the AD theater root and domain controllers/catalogs. It includes messaging services and management of Defense Message Service and Exchange.
- **Service Management Branch**. This branch implements the Service Management program for the TNOSC and the theater. It manages the Service Level and Operational Level Agreements that the TNOSC enters into. It monitors the theater Service level delivery program for the TNOSC/SC(T) and the subordinate units providing the SC(T) and commanders with SA of the service delivery across all disciplines of NETOPS. It provides performance management monitoring and reporting on the Information Technology Infrastructure Library capacity/availability areas and trending. The plans and engineering sections of the theater army G-6 and the signal command theater assistant chief of staff, operations (G-3) are customers of the performance analysis. This branch works 8 hours a day, 5 days a week.

NETWORK MANAGEMENT DIVISION

4-49. The Network Management Division operates and/or manages the underlying "transport" networks that other applications and services use. It is the focus on the underlying network that distinguishes it from the Enterprise Services Division. In some cases, the TNOSC operates a theater backbone and directs the operation of subordinate agencies in their operation of lower portions of the network. In other cases, it entirely directs the operations of subordinate units. A good example of this dichotomy is (the current day) DISA RNOSC/SC(T). It operates an IP backbone, but the Service/agencies operate the DSN backbone (OCONUS). The division consist of the following branches:

- **Data Networks Branch**. This branch provides oversight of the IP router networks (classified and unclassified). Operates the theater IP backbone. Provides oversight to operation of the IP networks by subordinate organizations. Provides theater level analyst functions, theater designs and access list architecture. Implements theater level IP reach back, to include routing plans, when the reach back is not to a STEP site. Reporting and SA of theater IP network capabilities. This branch operates 24 hours a day, seven days a week.
- **Switched Systems Branch**. This branch manages/operates the voice networks in theater, to include DSN and Defense Red Switch Network (DRSN). Actions performed by this branch include oversight of subordinate operating activities, validation of DISA implementation directives, CM of switches, integrating voice reach back and trunking, reporting and SA for voice capabilities within the theater. This branch operates 24 hours a day, seven days a week.
- **Transmission Systems Branch**. This branch operates/manages the transmission systems backbone, and oversees the operations of transmission systems by subordinate units. Examples of backbone systems operated include Fiber infrastructure, synchronous optical network, dense wavelength division multiplexing, asynchronous transfer mode (ATM), and integrated digital network exchange. Coordinates theater wide COMSEC re-keys. Oversees/tracks operation of satellite facilities by subordinate units. SA reporting for all transmission systems, to include deployed units. Depending on theater may also monitor circuits on STEP facilities (via "copy" feed of native management system). Implements routing plans. This branch operates 24 hours a day, seven days a week.

ENTERPRISE SYSTEMS MANAGEMENT DIVISION

4-50. This division manages the internal systems of the TNOSC (LAN, power, servers and operating systems) and devices distributed throughout the theater controlled by the TNOSC (such as DNS/RADIUS). The division consist of the following branches:

- **Systems Support and Integration Branch**. This branch provides support for the infrastructure and servers, with their accompanying operating systems. Notionally, this branch has a UNIX team, and Windows team, and a team that supports the infrastructure (switches, routers, virtual LAN configurations) as well as environmental concerns (power, A/C, server room management). The system administrators perform backups and coordinate this part (server restoral) of the COOP. Support for various operating system related tools, such as Citrix. They centrally manage patches and upgrades for the TNOSC controlled servers. This branch operates 8 hours a day, 5 days a week with on-call support.
- **Database and Applications Branch**. This branch operates and maintains the applications used by the TNOSC and distributed throughout the theater. A notional list would include: Remedy, Spectrum (or other network management systems), Formula, Tivoli, Oracle, Cricket/MRTG, ATM manager (supporting Remedy, as well as other applications such as CiscoWorks, CiscoSecure, et al). This team also integrates programs and provides interfaces to other agencies' systems (e.g. feeding status from Spectrum to DISA's integrated network management system). This branch also establishes the technical architecture for distributing these products and views throughout the theater. This branch operates 8 hours a day, 5 days a week with on-call support.

INFORMATION ASSURANCE DIVISION

4-51. The IA Division provides operational oversight of the IA aspects of the network. The division consist of the following branches:

- **Network and Systems Monitoring Branch**. This branch monitors the theater network sensor grid, including the IDS, other Top Level Architecture sensors, DID IDS sensors, host based IDS, (theater level) firewalls, etc. It provides detection, first level analysis (triage) and initial response, to include coordinating for blocking actions, trouble ticket initiation and dispatch. This branch is staffed 24 hours a day, seven days a week.
- **Information Assurance Branch**. This branch does the follow up, tracking, and reporting of incident tickets. Performs internal and directed external scans and reports. Designs and verifies ACL/firewall rule set. IAVA reporting for the TNOSC. Manages the theater software update services program (or other update service). Manages theater Anti-Virus update programs. Manages theater CAP registration. Oversees accreditation and security actions of subordinate units' IA personnel. Crosschecks patch levels and IAVA compliance for all TNOSC systems. This branch is staffed for 8 hours a day, 5 days a week with on-call support.

4-52. The TLT performs a liaison function to a corps, division, or brigade NETOPS cell that already exists. The TLT provides essential integration services between the tactical unit and the respective TNOSC. It also provides valuable technical NETOPS augmentation to the unit's organic NETOPS capability. When supporting a corps or division and a corps or division-based command, a TLT would typically collocate with appropriate personnel at the assigned sanctuary. TLT personnel in support of an expeditionary BCT may perform these functions from the TNOSC, or they may relocate to other locations as the mission dictates. A typical scenario for these elements is depicted in Figure 4-4.

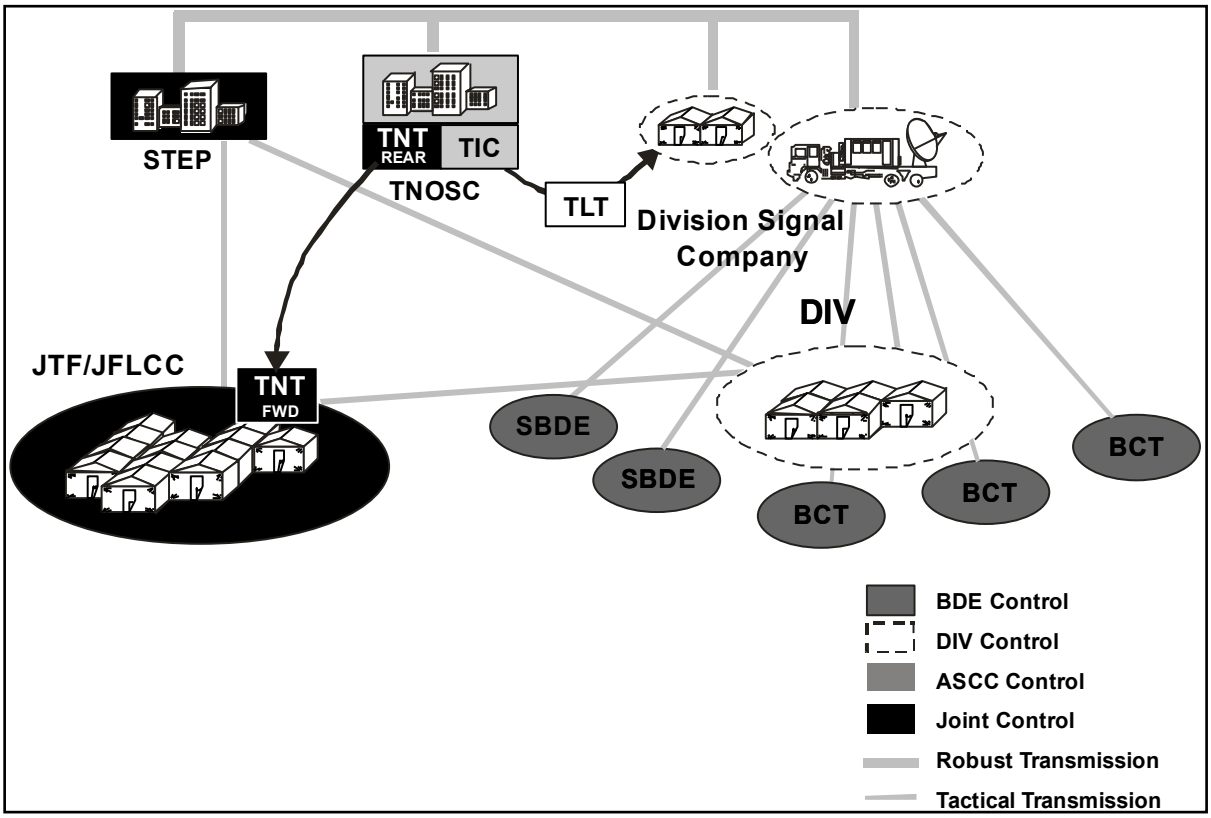

Figure 4-4. TNOSC deployment support division elements: TNT, TIC, and TLT

TACTICAL SIGNAL BRIGADE NETOPS

4-53. The SB(T) S-3 performs NETOPS functions for all subordinate ITSB/ESBs and other supported units. It also serves as the NETOPS interface to higher headquarters (e.g., it acts as a tactical NOSC). This includes operational planning in conjunction with the theater G-6 as well as detailed engineering of ITSB/ESB provisioned NETOPS capabilities.

INTEGRATED THEATER SIGNAL BATTALION NETOPS

4-54. The battalion S-3 element of the ITSB/ESB headquarters provides a NETOPS span of control function for the ITSB/ESB. The S-3 performs all NOSC functions necessary to manage and secure the ITSB/ESB network assets, and provide NETOPS capabilities and SA to the supported commander.

DIVISION NETOPS AND SECURITY CENTER

4-55. The division G-6 employs a fully integrated NOSC that provides NETOPS functions for the division G-6. The division signal elements must coordinate with the NOSC during the engineering, installation, operation, maintenance, and defense of the division information network.

4-56. Habitually, the division NOSC is co-located with one or more division TOCs. Due to recent enhancements to tactical reach operations capability, the division G-6 may elect to perform some or all NOSC functions from remote sanctuary locations such as the division tactical UHN or a division-controlled cell within the network service center regional. Performing NOSC functions at unit-controlled sanctuary locations is generally most effective during deployment and decisive operations. During these phases, the division TOC is highly mobile and cannot provide a stable high-speed environment to host AOR services.

4-57. The division NOSC, under the direction of the division G-6, has overall responsibility for establishing the division information network and provides the operational and technical support to all of the division signal elements in its AOR. The division NOSC performs the NETOPS activities, functions, and tasks required to quickly shift priorities in order to support the division commander's intent. Division NOSC responsibilities include:

- ICW the TNOSC, monitors, manages, and ensures implementation of ESM/NM, IA/CND, and IDM/CS activities (performed by the division G-6 and subordinate organizations).
- Provides near real-time awareness of division networks and systems to the division G-6 and higher headquarters' NOSC.
- Coordinates actions to resolve attacks or incidents on the division network with the TNOSC and subordinate organizations.
- Coordinates operational procedures and requirements for IA/CND and information systems security with the supporting TNOSC.
- ICW the TNOSC, monitors, manages, and controls intra-division information network components (performed by the division G-6).
- Monitors the operation of the networks in the division's subordinate brigades.
- Provides support and assistance to the subordinate NOSCs as required.
- Manages the organizational messaging system of record (Defense Message System, Tactical Message System) in the division, including managing network addresses and sub-domains.
- Coordinates operation and maintenance support of communications systems attached to support deployed division forces with the split-base and reach operations capability to the home base.
- Shares ESM/NM information with other management or monitoring centers.
- Provides the supporting TNOSC with near real-time information on the status and performance of inter-division networks.
- Orders and accounts for all forms of COMSEC material. This includes storing keys in encrypted form and performing key generation and automatic key distribution.
- Performs COMSEC material accounting functions and communicates with other COMSEC elements.
- Performs IDM/CS functions to support all aspects of relevant information dissemination.
- Provides near real-time awareness of all networks and systems within the division AOR.

BRIGADE NOSC

4-58. The brigade NOSC is the control center for the brigade network that manages all current operations and network configuration. The brigade NOSC reports directly to the brigade G-6. The brigade NOSC operates closely with the TOC nodal platoon, utilizing the JNN's organic network management capability to configure, monitor, and manage the WAN. The brigade NOSC supports the G-6 section in the planning, configuration, management, and monitoring of the TOC LANs as well as prioritizes the dissemination of information across the WAN. ICW the brigade G-6, the brigade NOSC—

- Coordinates, plans, and manages brigade frequency assignments.
- Plans and manages the brigade information network.
- Plans and manages all IA/CND operations to include, but not limited to, IA systems (firewalls, IDSs, and ACLs), key management distribution, IAVA compliance, and IDM and operations, and compliance with all directives outlined in AR 25-2.
- Plans and manages brigade IDM/CS procedures (user profiles, file and user priorities, and dissemination policies) (at higher headquarters' NOSC and supporting TNOSC).
- Evaluates network requirements to determine needs for brigades and communications relay requirements.
- Aides in the execution of all NETOPS responsibilities in support of the unit mission.

Note. To support the information in this chapter, Appendix G and H provides deployment scenarios for the division, BCT, and ASCC.

NETWORK OPERATIONS COMMAND AND CONTROL RELATIONSHIPS

4-59. The senior ARFOR mission commander commands and controls the tactical Army network in compliance with joint, Army, and theater NETOPS policy and direction. To ensure that a seamless and autonomous network is achieved, the mission commander delegates the authority to control and configure the network to the G-6 through the telecommunications service order (TSO) process.

4-60. For current operations, the G-6 coordinates network reconfigurations through technical channels based on the TSO process mentioned above and as specified by the commander in the operations order. These changes include frequency modification, router configurations, or equipment settings. When reconfiguration involves the movement of personnel and equipment within the current operation, the G-6 coordinates that adjustment with the G-3 and the G-3 issues the appropriate fragmentary order (FRAGO) in support of that reconfiguration.

4-61. For future operations, the G-6 participates in the military decision making process. He identifies the correct placement of network equipment and personnel on the battlefield in support of the mission. This information is then vetted through COA development and published in the unit OPORD and requisite signal annex.

4-62. The TSO process and technical channels are used for coordinating the configuration of the network. This process flows from the GCC J-6 through the JTF, combined joint force land component command, ARFOR, corps, division, BCT, and the battalion J-6, G-6, and S-6 structure to facilitate the establishment and health of the enterprise network and theater network.

4-63. NETOPS control is the authority granted to a senior signal officer and his staff from their immediate operational commander in compliance with joint, Army, and theater NETOPS policy and direction. This ensures the day-to-day compliance of their network with their associated LWN and GIG requirements. In addition, the fast moving nature of NETOPS, which is inherently a 24-hour/7-day operation, requires quick decisions and adjustments that exceed the responsiveness of the traditional orders process.

4-64. Through technical channels coordination and the TSO process, the signal officer and staff execute the commander's directives to maintain and secure their network. This process involves policy, guidance, and directives issued to subordinate signal organizations along the NETOPS channels. The TSO does not allow the commander's signal staff to move equipment or personnel but it does allow them to coordinate CM of network devices within their area of operations. If there is a need to move equipment or personnel in order to meet network requirements, the signal staff needs to coordinate with their respective G-3 or S-3 and issue a FRAGO to the existing signal annex of the operations order for movement.

4-65. It is important to remember the TSO is a current operations process. The TSO is designed to give the commander, through his signal staff, a means to adjust and modify the existing network plan to meet unexpected circumstances that can range from outright network attacks to system failures and service interruptions. Any future NETOPS control issues must be planned and executed through the orders process (military decision making process) performed by the chain of command.

4-66. Lastly, any time the signal staff receives a TSO from a higher signal entity, they conduct a review to determine if that TSO is potentially detrimental to their commander's mission priorities. If it is determined that the impact is not relevant to the mission, the signal staff then executes that TSO and informs the commander. If the potential exists, the implementation of that TSO will affect the mission; the signal staff coordinates with the command chain and requests guidance. If the decision is made by the commander not to execute the TSO, then the necessary coordination to deconflict any issues is performed between the command chain and the higher headquarters that issued the TSO.

Chapter 5

Network Operations Activities

This chapter provides the conceptual framework for the execution of NETOPS. It links organizations described in Chapter 3 and the phases and relationships described in Chapter 4. It also addresses methods to reduce forward-deployed NETOPS and global NETOPS policies and standards.

OVERVIEW

5-1. NETOPS activities were derived from the AENIA. They address the activities associated with the provisioning and management of NETOPS capabilities. The activities are organized into four major areas:

- **NETOPS policies, standards, planning, and design.** NETOPS policies and standards provide a common foundation and general guidance for the provisioning and management of NETOPS capabilities in support of the Soldier. NETOPS capabilities require planning and design to be effective regardless of the affected organization, system, or technology. Planning and design of NETOPS capabilities is especially important in the tactical environment with its potential for limited connectivity and the "fog of war" that can be experienced in the tactical environment.
- **Tactical operation of the network.** The activities in this area directly support the Soldier with NETOPS capabilities. This support spans all phases of operations. The NETOPS operational activity area comprises the majority of this chapter. These activity categories represent the best practices of NETOPS capability providers (both Army and industry) and provide a means of categorizing NETOPS capabilities that is not specific to any technology or organizational structure.
- **NETOPS evaluation**. The evaluation of NETOPS capabilities extends the infrastructure monitoring found in the operations activity area. It supports the monitoring and reporting of capacity, availability, and IA compliance. It is focused on the health and protection of the network and its services. It also provides the capability to support proactive management of NETOPS capabilities.
- **NETOPS training**. Effective use of NETOPS capabilities requires continuous training. As new or updated NETOPS capabilities enter the tactical environment, the skills of the Soldiers require enhancement or refreshment.

5-2. The descriptions of the activities in this chapter follow a common template. First, the NETOPS functional activity itself is defined and described. Next, the echelon(s) and organization(s) that support the specific activity are identified and details are provided on how organizations support the specific NETOPS activity. This support information includes the inter-organizational relationships associated with the specific NETOPS activity. Lastly, any joint implications related to the execution and support of the activities is identified.

NETWORK OPERATIONS POLICIES, STANDARDS, PLANNING, AND DESIGN

5-3. NETOPS policies and standards provide a common foundation and guidance for the provisioning of NETOPS capabilities to the Soldier. The NETOPS planning and design process encompasses the preparation required for the fielding and the continued support for NETOPS capabilities. Both global and temporary mission-specific policies and standards are addressed in this section.

GLOBAL NETOPS POLICIES AND STANDARDS

5-4. Global tactical NETOPS policies and standards, while approved and issued from the global Army and joint levels, apply to the provisioning of NETOPS capabilities at all tactical echelons. These policies and standards define general NETOPS-related system configurations, procedures, protocols, and information exchange requirements.

Note. Temporary changes to network policies can be more stringent or strict than the global policies but cannot be less stringent or strict.

5-5. Global NETOPS policies and standards enable compatibility between tactical elements and minimize the disruption caused by task organization. Global policies and standards are also critical in order to provide tactical units with strategic support services and to help ensure compatibility between units that come together from different geographical areas and different commands. Tactical units are partially dependent on support from non-tactical echelons due to physical and manpower limitations. To effectively provide strategic NETOPS support, the provisioning of tactical NETOPS capabilities must be performed in a uniform and well-defined manner. While global tactical NETOPS policies and standards define and support standardized NETOPS capabilities within tactical echelons, they do not impair the tactical commander's ability to dynamically manage and allocate NETOPS capabilities.

5-6. Some examples of global NETOPS policies and standards include:

- Protocols and port configuration guidelines.
- Inter-organization information exchange requirements.
- Change approval and change implementation responsibilities.
- Reportable CM information.

Note. Appendix C outlines a scenario of how policy management may occur.

Global NETOPS Policies and Standards in Echelons and Organizations

5-7. The primary responsibility of establishing global Army NETOPS policies and standards resides with the CIO G-6. Both NETCOM/9th SC(A) and the US Army Signal Center support the CIO G-6. Refinement of global policies with respect to tactical echelons is performed via direct interaction between theater policy-makers and the tactical echelons. Global policies and standards are continually reviewed and periodically updated based on policy and standards recommendations from tactical organizations, Army enterprise modularity and efficiency requirements, and relevant technological advancements.

Global Policies and Standards Joint Implications

5-8. A working relationship must be in place between Army NETOPS policymakers and the joint NETOPS community. Global tactical NETOPS policies initiated from the joint level require incorporation into global Army policy. Policies arising within the Army tactical community must also be considered by Army NETOPS policymakers through joint channels. This prevents policy conflicts when Army tactical elements are operating in a joint environment.

TEMPORARY EXCEPTIONS TO NETOPS POLICIES AND STANDARDS

5-9. Isolated changes or additions to NETOPS policies and standards threaten Army enterprise modularity and efficiency and should be minimized. NETOPS policies and standards in the tactical environment, due to the time-sensitive and volatile nature of tactical operations, cannot always adhere to the lengthy policy change process that is normally required in the fixed-station environment. Mission-specific factors may necessitate temporary additions or changes to policy.

5-10. Additions, changes, or exceptions to tactical NETOPS policy are approved via the chain of command as previously described in Chapter 4. Prior approval must be granted from the next higher headquarters if any particular echelon wishes to add, change, or circumvent tactical NETOPS policy. For example, if a BCT commander wishes to issue a policy stating that all subordinate units must block a particular network protocol, prior approval must be obtained from its higher headquarters, which will typically be a division. This approval process decreases the likelihood that a unit will issue guidance that will impair the functionality of the assets under its control or impact the broader NETOPS state of affairs. If the policy addition or change is likely to cause a decrease in overall network health or modularity, the approving headquarters will carefully consider whether the requirement for the policy change outweighs the potential impacts.

5-11. In some cases, a policy change or addition requires approval by an echelon higher than the requesting organization's parent headquarters. This is expected to occur when the policy change may cause immediate network-wide security or functionality ramifications. In the general case, echelons above the organization's parent headquarters only require notification when there is policy modification.

5-12. Exceptions to policy are forwarded through, and accumulated by, the chain of command. This data should be reviewed and used to provide recommendations for global Army NETOPS policy and standard changes and additions.

5-13. In any tactical scenario, there may be urgent situations where there is no time for an approval process before policy guidance must be issued. The unit commander (advised by the S-6, G-6, and J-6) will make this decision and take responsibility for any potential impact to the Army enterprise, both fixed and tactical.

Temporary Exceptions to NETOPS Policies and Standards in Echelons and Organizations

5-14. For the BCT and below, temporary exceptions to policies and standards are defined and maintained by the BCT S-6 personnel. These short-term exceptions to policies and standards are based on BCT mission requirements and refined from Army global policies and standards, as well as any other temporary mission-specific policies and standards implemented by echelons within the BCTs chain of command. The BCT provides policies and standards guidance to its AOR.

5-15. The corps and division G-6 personnel define and maintain temporary exceptions to policies and standards in support of the corps and division. These exceptions to policies and standards are based on the corps or division mission requirements and further refined from Army global policies and standards, as well as any other temporary mission-specific policies and standards implemented by echelons within the corps or division's chain of command. The corps and division provide exceptions to policies and standard guidance to its assigned AOR, including BCTs, ITSBs, ESBs and support brigades. The corps and division should also consider how changes might affect lateral or supporting organizations and the modularity of subordinate organizations.

5-16. The numbered Army NETOPS temporary exceptions to policies and standards are defined and maintained by the numbered Army G-6 personnel. These exceptions to policies and standards are based on the numbered Army's mission requirements from Army global, and potentially joint, policies and standards applicable within their theater. The numbered Army provides policies and standards guidance to its assigned corps and division, directly reporting BCTs and other theater assets. The ASCC must consider how any changes could affect NETOPS with other ASCC organizations and should be guided by policies and direction from the A2TOC.

Temporary Exceptions to NETOPS Policies and Standards Joint Implications

5-17. The ARFOR NETOPS mission specific policies and standards are defined and maintained by ARFOR G-6 personnel. These mission-specific policies and standards are based on ARFOR mission requirements and further refined from Army global standards as well as any other temporary mission-specific policies and standards implemented by echelons within the ARFORs chain of command. The ARFOR provides mission-specific policies and standards guidance to its assigned corps and division, BCTs, and other signal elements within its AOR. The ARFOR must carefully consider how policy changes

might affect lateral or supporting signal organizations and the modularity of subordinate corps, division, and BCTs.

5-18. Joint organizations within an Army organization's chain of command are expected to define and maintain organizational and mission-specific NETOPS policies and standards. Joint organizational and mission-specific policies and standards are created and approved through the joint operational environment chain of command.

5-19. Army tactical organizations will incorporate joint and global Army tactical NETOPS policies and standards just as they would if their parent headquarters was an Army organization. If Army and joint NETOPS policies or standards conflict, the organizational S-6, G-6, and J-6 will notify their joint and Army parent headquarters. The clarification of conflicting policies and standards is the responsibility of their chain of command.

NETOPS MISSION PLANNING

5-20. NETOPS mission planning is the collection of current and future user requirements, requirements validation and prioritization, mission alignment to the commander's intent, the allocation of technical and organizational resources, and the publication of operation orders. Major NETOPS mission planning is normally performed during the first phase of the operation. Because of some system transmission delays that are inherent in some SATCOM equipment, one example of mission planning is to allocate tropospheric scatter capability to a user instead of a SATCOM. Smaller scale mission planning is performed in all phases of operations as dictated by mission requirements.

Mission Planning Echelons and Organizations

5-21. All organizations in the tactical chain of command are involved in the NETOPS mission planning process. As each echelon of the tactical chain of command performs mission planning, guidance is given to subordinate echelons. This guidance is then used to create or refine NETOPS mission planning at the lower echelon. Mission planning is a continual process that is performed by the organization's S-6, G-6, and J-6 staff.

5-22. For the BCT and below, NETOPS mission planning is performed by the BCT S-6. The BCT provides mission planning support to subordinate maneuver battalions.

5-23. The corps and division G-6 performs NETOPS mission planning in support of the corps and division. The corps and division provide mission planning guidance to assigned BCTs and support brigades as well as coordinating mission planning efforts between its subordinate BCTs and support brigades.

5-24. For the numbered Army, NETOPS mission planning is performed by the numbered Army G-6. The numbered Army provides mission planning guidance to assigned corps and divisions, directly reporting BCTs, and support brigades. The numbered Army also coordinates mission planning efforts between its subordinate organizations. The numbered Army G-6 also coordinates with the signal command (theater) (SC[T]) during this planning process.

5-25. During mission planning and especially during Phase One, coordination may be required between theaters. The numbered Army will perform inter-theater coordination in support of deploying or re-deploying organizations.

Mission Planning Joint Implications

5-26. Mission planning is performed by the joint and Army operational environment chain of command. The joint chain of command will participate in the activities as described. Army tactical organizations will incorporate joint mission planning guidance as they would should their parent headquarters be an Army organization. If the Army and joint NETOPS mission planning guidance conflict, the organizational S-6, G-6, and J-6 will notify their joint and Army parent headquarters. The clarification of conflicting guidance is the responsibility of their chain of command.

NETOPS CAPABILITY DESIGN

5-27. NETOPS capability employment configuration is usually performed in response to the receipt of planning information in the form of OPORDs and annexes related to the accomplishment of a specific mission. NETOPS capability employment configuration supports and provides feedback to the mission planning activity described in this chapter. NETOPS employment configuration is defined to include—

- Development of operational configurations to provide the required IT mission support capability. Tactical NETOPS capability employment configuration includes development of configurations for communications, networks, systems, and security capabilities in support of Soldier NETOPS.
- Development of operational configurations required to facilitate the internetworking of NETOPS-related applications, systems, networks, and communications infrastructure.

Capability Employment Configuration Echelons and Organizations

5-28. The tactical environment where NETOPS capability employment configuration is performed depends on the echelon providing the NETOPS capability, the means by which the capability is provided, the echelon to which the capability is being provided, and the NETOPS capability being employed. For example, in electromagnetic spectrum operations, most echelons are required to identify what frequency resources will be required and where they will be used within frequency management (sometimes referred to as spectrum management), most echelons are required to identify what frequencies will be used and where they will be used within their AOR. In other scenarios, electronic messaging may not require capability employment configuration below the corps or division level.

5-29. All organizations in the tactical chain of command are involved in the NETOPS capability employment configuration, either directly or in a coordinating or supporting role. As each echelon of the tactical chain of command performs NETOPS capability employment configuration, information is provided to subordinate echelons. The echelon that begins the employment configuration process for a particular system is the highest echelon that must integrate the system across multiple subordinate units. The employment configuration process then extends down to the echelon that maintains operational management of the system in question (refer to operational control and management process for further details). This information is then used to create or refine NETOPS capability employment configuration at the lower echelon. NETOPS capability employment configuration is performed by the organization's S-6, G-6, and J-6 staff.

5-30. For the BCT and below, NETOPS capability employment configuration is performed by the BCT S-6. The BCT provides capability employment configuration support to subordinate maneuver battalions.

5-31. For the corps and division, NETOPS capability employment configuration is performed by the corps and division G-6. The corps and division provide capability employment configuration guidance to its AOR, including assigned ITSBs/ESBs, BCTs, and support brigades. The corps and division coordinate capability employment configuration efforts between their subordinate BCTs and support brigades. Corps and division capability employment configuration is focused on facilitating the interoperability of the NETOPS capabilities between echelons.

5-32. For the numbered Army, NETOPS capability employment configuration is performed by the numbered Army G-6. The numbered Army provides capability design guidance to assigned corps, divisions, and directly reporting BCTs. The numbered Army coordinates capability employment configuration efforts between its subordinate organizations. The numbered Army G-6 also coordinates with the SC(T) in this capability employment configuration process. The numbered Army's capability employment configuration is focused on facilitating the interoperability of the NETOPS capabilities between echelons.

5-33. During capability employment configuration, and especially during Phase One, coordination may be required between theaters. The numbered Army will perform inter-theater coordination in support of deploying or redeploying organizations.

Capability Employment Configuration Joint Implications

5-34. The ARFOR NETOPS capability employment configuration is performed by the ARFOR G-6. The ARFOR provides capability employment configuration guidance to its AOR. This includes assigned corps, division, ITSB/ESB, BCTs, and support brigades. The ARFOR also coordinates capability employment configuration efforts between subordinate assets within its AOR. ARFOR capability employment configuration is focused on facilitating the interoperability of the NETOPS capabilities between echelons and provisioning services to meet mission requirements.

5-35. Tactical NETOPS capability employment configuration is performed by the joint and Army operational environment chain of command. The joint chain of command will participate in the NETOPS capability employment configuration in support of assigned Army organizations. Army tactical organizations will incorporate joint capability employment configuration guidance as they would should their parent headquarters be an Army organization. If the Army and joint NETOPS capability employment configuration guidance conflict, the organizational S-6, G-6, and J-6 will notify their joint and Army parent headquarters. The clarification of conflicting guidance is the responsibility of their chain of command.

TACTICAL OPERATIONS

5-36. Tactical operations are the NETOPS activities that frame the management, support, execution, and evaluation processes required to provide a stable NETOPS infrastructure to support the tactical LWN. These activity categories represent the best practices of NETOPS capability providers (both Army and industry). They also provide a general means of categorizing NETOPS capabilities that are not specific to any technology or organizational structure. The following paragraphs discuss these NETOPS activities.

NETOPS REPORTING

5-37. The corps, division, and numbered Army level organizations are required to provide day-to-day SA of Army network and system reports in their AOR to the senior tactical commander and the TNOSC. NETOPS reporting identifies critical network outages, availability, integrity, and confidentiality of the LWN.

5-38. The A-GNOSC will publish Army NETOPS reporting requirement in an OPORD. Army NETOPS OPORD 05-01, dated 20 April 2005, delineates NETOPS reporting threshold guidelines for post, camp, and station service providers (tactical and strategic); TNOSCs; and the A-GNOSC. The thresholds identified are considered baseline criteria only; service providers or unit commanders may modify the baseline to allow for more stringent reporting criteria as deemed necessary.

Reporting Joint Implications

5-39. When the numbered Army is not acting as the joint operational area ARFOR, the ARFOR has a dual NETOPS reporting requirement to its joint command and to its local numbered Army. NETOPS reporting responsibilities to a joint command are determined by the joint community (reference JP 6-0). NETOPS reporting responsibilities between the ARFOR and the numbered Army should be performed according to the guidelines listed above.

NETOPS SHARED SA PICTURE

5-40. The requirement for NETOPS shared SA was established in the August 2000 Deputy Secretary of Defense-DOD CIO Guidance and Policy Memorandum No. 10-8460 Network Operations, which mandated a network common operating picture (NETOPS shared SA). Detailed descriptions of the execution of this requirement are found in the current joint NETOPS concept of operations (CONOPS), which directs a shared, single integrated network SA view for the GIG and, specifically, for the Army. The Army NETOPS CONOPS further directs a NETOPS shared SA that will display relevant NETOPS information to Army commanders to assist in identifying "...outages and degradations, network attacks, mission impacts, communications system shortfalls, operational requirements, and problem resolutions at the strategic,

operational, and tactical levels." This integrated, near-real-time picture tracks critical systems and designated high priority applications via views that are relevant to the specific information consumer (e.g., A-GNOSC, CCDR, numbered Army, TNOSC, corps, and division).

5-41. The NETOPS shared SA activity involves the collection of data from various LWN sources. These sources provide OPORD 05-01 defined reportable situations (outages, hazardous conditions information records, aggregated near real-time network event data from multiple network management toolsets, and data from other NETOPS shared SA systems). The collected data is then transformed into relevant information for a specific consumer or set of consumers and published as a view. Each consumer requesting a NETOPS shared SA view has the ability to customize the presented information to make it relevant to their situational requirements. In this manner it is envisioned that this common source of theater NETOPS shared SA information will allow any user on the network to pull only what is needed at the time. Figure 5-1 provides a high-level overview of the current NETOPS shared SA architecture developed and shared by the AGNOSC/TNOSC.

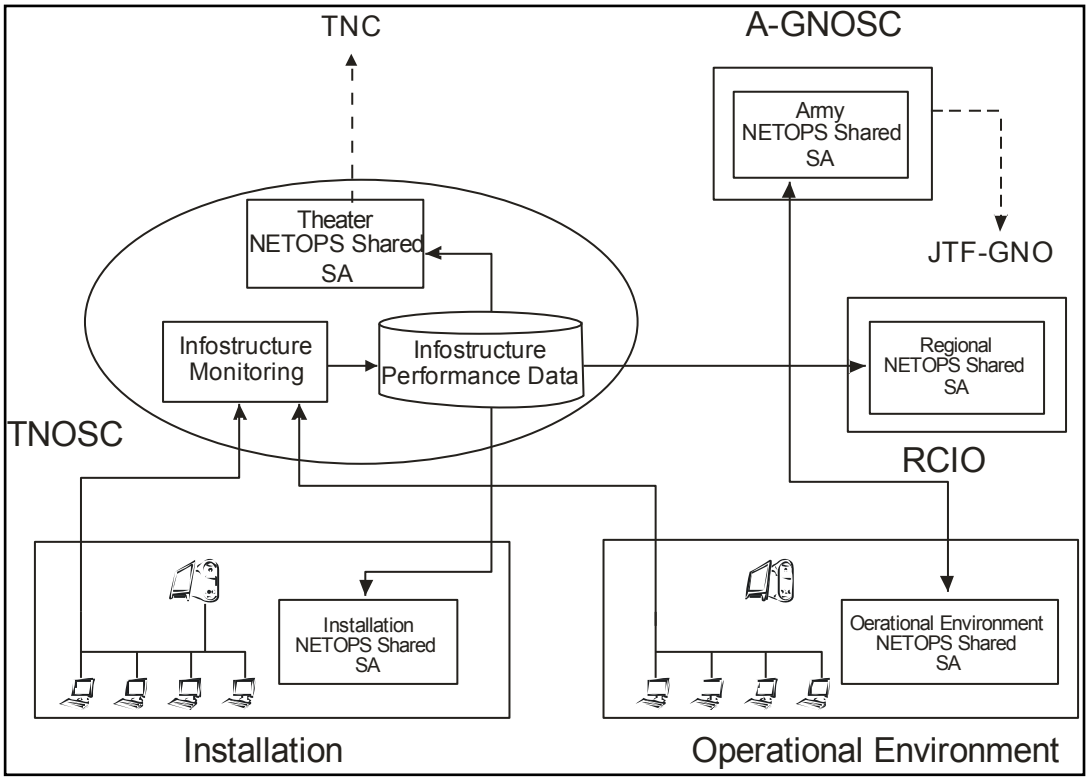

Figure 5-1. NETOPS shared SA system overview

Shared SA Echelons and Organizations

5-42. The BCT is responsible for ensuring the relevant systems within its AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC. A BCT may be a consumer of NETOPS shared SA information, but the NETOPS shared SA view would be provided by the TNOSC.

5-43. The corps and division is responsible for ensuring the relevant systems within its AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC. A corps and division may be a consumer of NETOPS shared SA information, but the NETOPS shared SA view would be provided by the TNOSC. The larger a corps or division's AOR, the more likely it would be a NETOPS shared SA consumer.

5-44. The numbered Army is responsible for ensuring the relevant systems within its AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC. The TNOSC will aggregate the data for the entire theater AOR and transform the data into presentable NETOPS shared SA information. The TNOSC then publishes a NETOPS shared SA view for consumer organizations. The TNOSC also reports aggregated NETOPS shared SA data for the theater to the A-GNOSC.

5-45. It is within the TNOSC's purview to provide a NETOPS shared SA to any eligible consumer that makes the request. In this respect, the TNOSC is the sole provider of the theater NETOPS shared SA. NETOPS shared SA support for the theater will come from the TNOSC due to the centralization of NETOPS shared SA activities at the TNOSC.

Shared SA Joint Implications

5-46. Upon request, the TNOSC will provide a NETOPS shared SA picture to ARFOR NOSCs, joint force land component commanders (JFLCCs), JTFs, JNCCs, theater NETOPS centers, and TNCCs. It is important to note that the deployed joint and Army communities will have different focuses and be interested in tracking different information. For example, while the Army is interested in the overall health of its NETOPS capabilities, the joint community will be focused on the warfighting situation. NETOPS shared SA will be essential to the JTF's ability to quickly assess and react to capability degradations that potentially impact its warfighting ability.

NETOPS CHANGE MANAGEMENT

5-47. The goal of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all modifications. This will help facilitate necessary changes and minimize the negative impacts of change-related events. The process encompasses the identification, documentation, approval, and implementation of variances from configuration baselines requirements.

5-48. Change management activities concerning user systems and NETOPS capabilities are generally performed by the unit's S-6, G-6, and J-6. Some of the activities concerning the network and basic network capabilities are provided by the supporting signal unit such as the division, brigade, and BCT signal company, the TLTs (BCT, corps, and division), or the ITSB ESB and TNT (numbered Army, ARFOR, and above).

5-49. The change management process is initiated by a request for change. A request for change may originate from any organization within the tactical chain of command, as well as the A-GNOSC or numbered Army. Requests for changes may be initiated as a resolution to an incident or problem, to request temporary exceptions to policies, or to support other emerging mission requirements.

5-50. Once a request for change is submitted, it enters the change processing state and is sent up through the tactical chain of command until it reaches the appropriate echelon to approve the change. As the change request is forwarded, it must pass through each intermediate echelon of tactical command. This ensures that the chain of command is aware of all requests and that approved changes are implemented in an orderly manner. At each echelon, the change must be examined by plans and engineering personnel. The reviewing stage is necessary to ensure that the change is feasible, justified, and does not violate network, system, or security policy guidance.

5-51. Change approval authority is based upon operational management responsibilities as defined in the NETOPS Operational Control and Management section later in this chapter. If an echelon has operational management of a particular system, it also has the authority to approve changes to that system, as long as these changes do not violate policy or guidance. If the request for change violates current policies or guidance, the change request must be processed as a temporary exception to policy (refer to the Temporary Exceptions to NETOPS Policies and Standards Section earlier in this chapter).

5-52. The unit commander will generally delegate the authority to approve or deny network change requests to the S-6, G-6, and J-6 command staff. This authority may be institutionalized or delegated to

technical network personnel within the unit. Qualified personnel include members of a signal company, ITSB/ESB, or supporting TLT.

5-53. After the echelon with the necessary authority has approved the change, the validated change request will pass to the echelon(s) with change implementation responsibility for the system(s) affected. This echelon will then coordinate the change with all necessary organizations before execution. An organization requires prior change coordination if the change may result in failure or the compromise of services within the organization's AOR.

5-54. Changes may also be initiated by high level echelons such as the CCDR or A2TOC. For example, a system may urgently require a patch based upon a newly identified vulnerability. Change requests originating at the CCDR are not required to go through the change approval process, but coordination with the ARFOR and affected tactical units is necessary to determine when and how the change should be implemented. Change requests originating from the A2TOC must be passed via the numbered Army to the ARFOR for approval. If the ARFOR determines that a change originating from the CCDR or A2TOC will have an unacceptable risk of disrupting user services, it can request to delay or defer the change through its chain of command.

5-55. Change implementation should always be performed by the echelon with operational management of the system in question. The NETOPS Operational Change and Management section in this chapter contains a general definition and delineation of operational management. In the tactical networking environment, situations will commonly arise that require immediate action to be taken. In these emergency situations, personnel may need to perform change implementation activities that are outside of their normal scope of responsibility.

5-56. Changes made to user systems, NETOPS capabilities, and network capabilities often involve configuration changes. These changes include updates to software, modifications to configuration parameters, and the replacement of hardware. Changes that are made within the network are recorded as they occur in an automated CM system. This system will provide notification to the appropriate organizations regarding any configuration modifications resulting from change requests. All units, BCT and above within the tactical network chain of command will have access to this system. Army organizations such as the numbered Army and A-GNOSC will also receive notification of configuration changes in order to maintain Army-based awareness across the enterprise.

Note. Change and CM are integrated activities. Specifically, changes to a configuration must be recorded through the CM activity. Appendix C contains scenarios that serve as examples of how change and CM occur.

Change Management Echelons and Organizations

5-57. NETOPS change management operations for assets within the BCT AOR are performed by the BCT S-6, supported by the BCT signal company, and assigned or attached signal personnel. At the BCT and below, each change request is approved, denied, or escalated to the next higher headquarters for further processing. The BCT performs change implementation on all systems for which it has operational management responsibility as defined in the Operational Control and Management Section of this chapter.

5-58. NETOPS change management operations for assets within the corps and division AOR are performed by the corps and division G-6, supported by the corps and division signal company, supporting TLT, and assigned or attached signal personnel. Each change request is approved, denied, or escalated to the next higher headquarters for further processing. The corps and division perform change implementation on all systems for which it has operational management responsibility as defined in the Operational Control and Management section of this chapter.

5-59. The ITSB/ESB performs designated change management functions in support of the echelon to which it is currently assigned. It will process and initiate change requests regarding the active NETOPS

capabilities it provides. The ITSB/ESB may also be delegated the authority to approve certain change requests from the supported S-6, G-6, or J-6.

5-60. The numbered Army and A-GNOSC perform all change management functions listed above for the support Services which are provided to the tactical forces via the TNOSC and A-GNOSC. The numbered Army or A-GNOSC receives and approves change requests regarding Army supporting services through the chain of command. The implementation of this change must be coordinated through all affected organizations as defined in the change implementation process. For example, a BCT under the OPCON of a corps or division may directly request a change to TNOSC support services through its corps or division.

Change Management Joint Implications

5-61. Joint guidance governs change management operations within joint organizations or between Army and joint organizations. Army personnel supporting these functions will operate within joint guidance while also utilizing Army change management procedures.

5-62. NETOPS change management operations for assets within the ARFOR AOR are performed by the ARFOR G-6, supporting ITSB/ESBs, and assigned or attached signal personnel. At the ARFOR, each change request is approved, denied, or escalated to the next higher headquarters J-6 for further processing. The JFLCC and commander, joint task force (CJTF) perform change approval activities for all joint-managed systems that require approval above the corps and division level. The ARFOR performs change implementation on all systems for which it has operational management responsibility as defined in the Operational Control and Management section of this chapter. The ARFOR, JFLCC, and CJTF will also be fully involved in the change notification process for all assets within their respective AORs.

NETOPS CONFIGURATION MANAGEMENT

5-63. NETOPS CM supports the identification, control, maintenance, and verification of systems and devices associated with the provisioning of NETOPS capabilities. Configuration item (CI) information includes hardware, software, device configurations, and version information. Activities associated with CM include:

- Identification of all CIs.
- Control of CIs.
- Maintenance of current and past CI status.
- Verification of CI status.

5-64. Policy dictates what qualifies as a CI and what information regarding each CI must be collected and stored. Policy also dictates how often CI information must be updated based upon mission factors including operational tempo and bandwidth constraints.

5-65. CM concerning user systems and capabilities are primarily performed by the unit's S-6, G-6, and J-6 staff. CM activities concerning the network and basic network capabilities are delegated to a supporting signal unit such as the signal company or the ITSB/ESB.

Configuration Management Echelons and Organizations

5-66. It is the responsibility of each echelon to ensure that all subordinate assets within its AOR perform the necessary CM activities. Each echelon in the tactical chain of command will ensure that CIs within subordinate echelons are accurately reflected within the CI database. To facilitate this process, read-only access of all network resources will be shared between designated network management personnel within each echelon.

5-67. An authoritative theater Army CI database (in support of the global Army CI database) will be maintained in a distributed fashion by the numbered Army TNOSCs.

5-68. For the BCT and below, CM operations are performed by the S-6 personnel, the signal company, supporting ITSB/ESBs, and supporting signal organizations. During the operational phases, all personnel

supporting NETOPS functions are required to ensure that CIs under their operational management are accurately identified and maintained within the CI database. When the BCT is task organized under a particular corps, division, or ARFOR, the BCT CI information is made available to the joint operational area chain of command and the gaining numbered Army. The BCT and below is also responsible for ensuring that all changes to systems under the operational control and management of the BCT are accurately reflected within the CI database.

5-69. Within the corps and division, CM operations will be performed by G-6 personnel, the signal company, supporting ITSB/ESBs, the TIC, and supporting signal organizations. During the operational phases, all personnel supporting NETOPS functions are required to ensure that CIs under their operational management are accurately identified and maintained within the CI database. This information can then be made available to the joint operations area ARFOR and the numbered Army as the corps or division deploys. The corps, division, and subordinate units are also responsible for ensuring that all changes to systems under their operational control and management are accurately reflected within the CI database.

5-70. Tactical CM operations are also performed by the ITSB/ESB on behalf of the supported tactical organizations. ITSB/ESBs will ensure that CIs under their operational management and those of their supported organization are identified and maintained accurately within the CI database throughout all operational phases. This information can then be passed from the owning numbered Army to various tactical echelons as the ITSB/ESB is task reorganized.

5-71. For the numbered Army's tactical support services, CM operations will be performed by the SC(T) and TNOSC. All personnel supporting NETOPS functions are required to ensure that CIs under their control are identified and maintained accurately within the CI database throughout all operational phases. The numbered Army is also responsible for ensuring that all changes to systems under the operational control and management of the numbered Army are accurately reflected within the CI database.

5-72. It is important to remember that one echelon may be responsible for a physical CI but not the CI's device configuration. For example, the BCT is responsible for ensuring that all its routers are entered or removed from the CI database. The BCT's higher headquarters, as the echelon with operational management of the BCT routers, is responsible for maintaining the status of router configurations within the CI database.

Configuration Management Joint Implications

5-73. The ARFOR, JFLCC, and CJTF CM operations are governed by joint guidance. Army personnel supporting these organizations will operate within this guidance while also utilizing Army CM procedures to the fullest possible extent. Army assets within these organizations will utilize the Army-provided CI database unless otherwise directed. Joint organizations will have the ability to view information from this database as required.

5-74. CM functions within the ARFOR, JFLCC, and CJTF are anticipated to be performed by the G-6, J-6, TNT, the supporting ITSB/ESB, and supporting signal organization. During the operational phases, all personnel supporting Army-based NETOPS functions should ensure that CIs under their operational management are accurately identified and maintained within the CI database. The ARFOR is also responsible for ensuring that all NETOPS changes to systems under the operational management of the ARFOR or subordinate Army elements are accurately reflected within the CI database.

NETOPS Incident and Problem Management

5-75. The incident and problem management process involves the processing and resolution of any event that is not part of the standard operation of a NETOPS capability, and that causes or may cause an interruption to or a reduction in the quality of that capability.

5-76. The goal of the incident and problem management process is to restore normal operation of the capability as quickly as possible, and minimize the adverse impact on tactical operations, therefore ensuring that the best possible levels of capability quality, availability, and security are maintained.

5-77. Management of network related incidents and problems concerning user systems and capabilities are the responsibility of the unit S-6, G-6, and J-6 staff. Incidents and problems concerning the network and basic network capabilities may be delegated to a supporting signal unit such as the signal company, TLT (BCT, corps, and division), or the ITSB/ESB and TNT (numbered Army or ARFOR).

Note. Appendix C outlines a scenario that serves as an example of how the incident and problem management activity might occur.

Incident and Problem Management Echelons and Organizations

5-78. For the BCT and below, incident and problem management operations are performed by the S-6, signal company, supporting ITSB/ESBs, and supporting signal organization. When an incident is identified within the BCT, it is first analyzed within the BCT to identify if an immediate resolution can be found. In the echelons BCT and below, the ability to locally analyze incidents is very limited. If a solution cannot be locally identified, the problem escalates to the next higher headquarters.

5-79. Within the corps and division, incident and problem management operations are performed by the G-6, signal company, supporting ITSB/ESB, TLT, and supporting signal organization. When an incident is identified within or escalates to the corps or division from a subordinate organization, it is first analyzed within the corps or division to identify if an immediate resolution can be found. If a solution cannot be locally identified, the problem escalates to the next higher headquarters within the tactical chain of command.

5-80. The ITSB/ESB personnel perform incident and problem functions for network capabilities and infrastructure provided by the ITSB/ESB. When an incident or problem is identified, it is first analyzed by ITSB/ESB NETOPS personnel to identify if an immediate resolution can be found. If a solution cannot be locally identified, the problem escalates to the supporting tactical echelon.

5-81. The numbered Army performs incident and problem management activities for all NETOPS capabilities provided by the numbered Army. If a tactical incident or problem cannot be resolved through local numbered Army resources, the numbered Army may escalate the problem to the A-GNOSC, material developer, or vendor subject matter experts.

5-82. The ultimate responsibility for tactical incident and problem management resides within the operational chain of command. Army organizations such as the TNOSC and the A-GNOSC play an important supporting role in this process. The deployment support division, within the TNOSC, supports tactical troubleshooting functions by leveraging a database of problems, incidents, and fixed-station subject matter experts. Tactical Army organizations may request support from the TNOSC or A-GNOSC through the chain of command.

Incident and Problem Management Joint Implications

5-83. Within the ARFOR, incident and problem management operations will be performed by the G-6, supporting ITSB/ESB, TNT, and supporting signal organization. When an incident is identified within or escalates to the ARFOR via a subordinate organization, it is first analyzed to identify if an immediate resolution can be found. The ARFOR will normally be supplemented by a numbered Army TNT in order to augment its ability to analyze incidents and problems. If a solution cannot be locally identified, the problem then escalates to the numbered Army TNOSC or the joint NETOPS cell within the JFLCC or CJTF.

5-84. The ARFOR will generally request assistance from the numbered Army's TNOSC to resolve problems related to Army-specific systems and procedures. Problems related to systems and procedures directly managed by the operational environment joint command will generally escalate to the joint NOSC. These problems can also be referred to the TNOSC at the discretion of the ARFOR. Regardless of escalation sequence, both the TNOSC and the combat chain of command will be notified of all incidents and problems as they occur.

5-85. The ARFOR, JFLCC, and CJTF incident and problem management operations are governed by joint guidance. Army personnel supporting these organizations will operate within this guidance while also participating in Army incident and problem management procedures to the fullest extent.

NETOPS RELEASE MANAGEMENT

5-86. Release management deals with the planning, design, construction, configuration, and testing of hardware and software to create a set of release components for a live environment. Release management activities also cover the planning, preparation, and scheduling of a release to various subscribers and locations.

5-87. The initiation, planning, and testing of releases are primarily performed in the fixed-station, non-tactical environment. It is critical that release building and testing are performed with the tactical environment in mind. This section provides details regarding those activities which are specific to the tactical echelons: release rollout planning, installation, and training.

5-88. The activities associated with release rollout planning are executed according to the change management and planning processes. When a release is issued, it is initiated as a change request. This request is then coordinated and planned through the tactical chain of command and all affected organizations.

5-89. The activities associated with release installation are executed according to change management guidelines. The echelon responsible for change management of the effected system(s) will execute the release.

NETOPS SERVICE DESK MANAGEMENT

5-90. Tactical service desk management encompasses all activities involved with tracking NETOPS activities, gathering NETOPS status or performance information, and interfacing with the tactical subscriber. This includes incident and problem processing, change request processing, availability management, user interaction, and collection of user satisfaction data. These activities are often associated with a user help desk.

5-91. Service desk management functions concerning user systems and NETOPS capabilities are the responsibility of the unit's S-6, G-6, and J-6 staff and functional areas. Service desk management functions are assigned, as necessary, by the S-6, G-6, and J-6 to a supporting signal unit such as the signal company or the ITSB/ESB.

Service Desk Management Echelons and Organizations

5-92. At the BCT and below, service desk management functions are performed in support of local subscribers. The service desk management information is collected, analyzed, and made available to the G-6 or J-6 within the next higher echelon.

5-93. Within the corps and division, service desk management functions are performed in support of local subscribers. The service desk management information is collected, analyzed, and made available to the G-6 or J-6 of the next higher commanding echelon.

5-94. Personnel performing service desk management functions within the corps, division, and below are likely to be network design, engineering, or incident management personnel with additional service desk management duties. In the upper echelons such as the ARFOR, numbered Army, and joint commands, service desk management functions will often be performed by dedicated personnel from a service management desk or help desk.

5-95. The ITSB/ESB will perform service desk management functions for the NETOPS infrastructure and all related capabilities provided by the ITSB/ESB. This information will be made available to the supported echelon and the local numbered Army.

5-96. The numbered Army will perform service desk management functions for all tactical support services provided by the SC(T) or TNOSC. This information will be made available to tactical Army units and the JTF.

Service Desk Management Joint Implications

5-97. Within the ARFOR, service desk management operations will be performed by the G-6, supporting ITSB/ESB, TNOSC TNT, and supporting signal organizations.

5-98. The JFLCC and CJTF service desk management operations are governed by joint guidance. Army personnel supporting these organizations will operate within this guidance while also performing Army service desk management procedures.

NETOPS INFRASTRUCTURE MONITORING/MANAGEMENT

5-99. NETOPS infrastructure monitoring is the monitoring of all IT components that are providing NETOPS-related capabilities to the Soldier. Monitoring is focused on the health of NETOPS capabilities. Some of these components include radios, multiplexers, cryptographic devices, routers, switches, firewalls, IDSs, enabling protocols, capability providing hosts, and critical applications.

5-100. NETOPS infrastructure monitoring is performed continuously throughout all phases of operations. It supports and enables other NETOPS operational activities such as NETOPS shared SA, service desk management, and incident and problem management.

5-101. Due to the complex nature of the Army's modular infrastructure, which consists of multiple Army NETOPS provisioning organizations, the monitoring of Army infrastructure components will be distributed among those organizations. Critical information collected by distributed NETOPS monitoring systems will be forwarded to a higher level NETOPS monitoring system. The concept of distributed monitoring is facilitated through the establishment of distinct monitoring domains, which are purposely aligned with the Army theaters' NETOPS provisioning organizations. The ARFOR, numbered Army, corps, division, BCT, and battalion organizations monitor their own domain as established in the NETOPS mission plan.

5-102. Each organization's monitoring domain consists of both the IT components within their AOR and the distant end of the WAN links to directly higher and directly subordinate organizations. For example, a corps or division monitoring domain would consist of all the IT components within its AOR as well as the distant ends of WAN links to the ARFOR (higher organization), adjacent units, ITSB/ESBs, and its BCTs (subordinate organization). In most situations, there will be line of sight and other WAN connections within an organization's monitoring domain that provide connectivity to distant entities of that organization. In this situation, all the IT components on the distant end of a particular WAN link are still under the monitoring responsibility of that organization.

5-103. In a dynamic combat scenario, there may be ad hoc Army, joint, coalition, or civilian assets attached to a BCT, corps, division, or ARFOR AOR. When this occurs, monitoring functions for these attached assets are the responsibility of the supported command. If the attached asset has the capability to perform independent monitoring activities, such as an ITSB/ESB or Marine expeditionary force, this asset would simply forward the monitoring data to the supported command. If not, the supported command would assume active, real-time monitoring of the attached asset.

5-104. Tactical units also require limited visibility of adjacent and higher networks for SA and troubleshooting purposes. A high-level view of the network as a whole can be obtained via remote network views provided by higher headquarters. For example, if a BCT needs to identify why communications to a remote ITSB/ESB are not functioning, it could access the Web view of the theater AOR which is available as a service via the TIC of the numbered Army's supporting TNOSC. Figure 5-2 illustrates the concept of distributed monitoring and the flow of the monitoring information.

Infrastructure Monitoring/Management Echelons and Organizations

5-105. For the BCT and battalion, infrastructure monitoring activities are performed by the S-6, signal company, supporting ITSB/ESBs, and other supporting signal organizations. These organizations will use their NETOPS monitoring system to monitor, manage, and troubleshoot the network infrastructure within their AOR. The battalion will provide all monitoring information from its AOR to the BCT. This information will consist of network topology, as well as event and alarm data. This provides the BCT with a read-only view of the battalion's infrastructure that will facilitate troubleshooting and analysis activities.

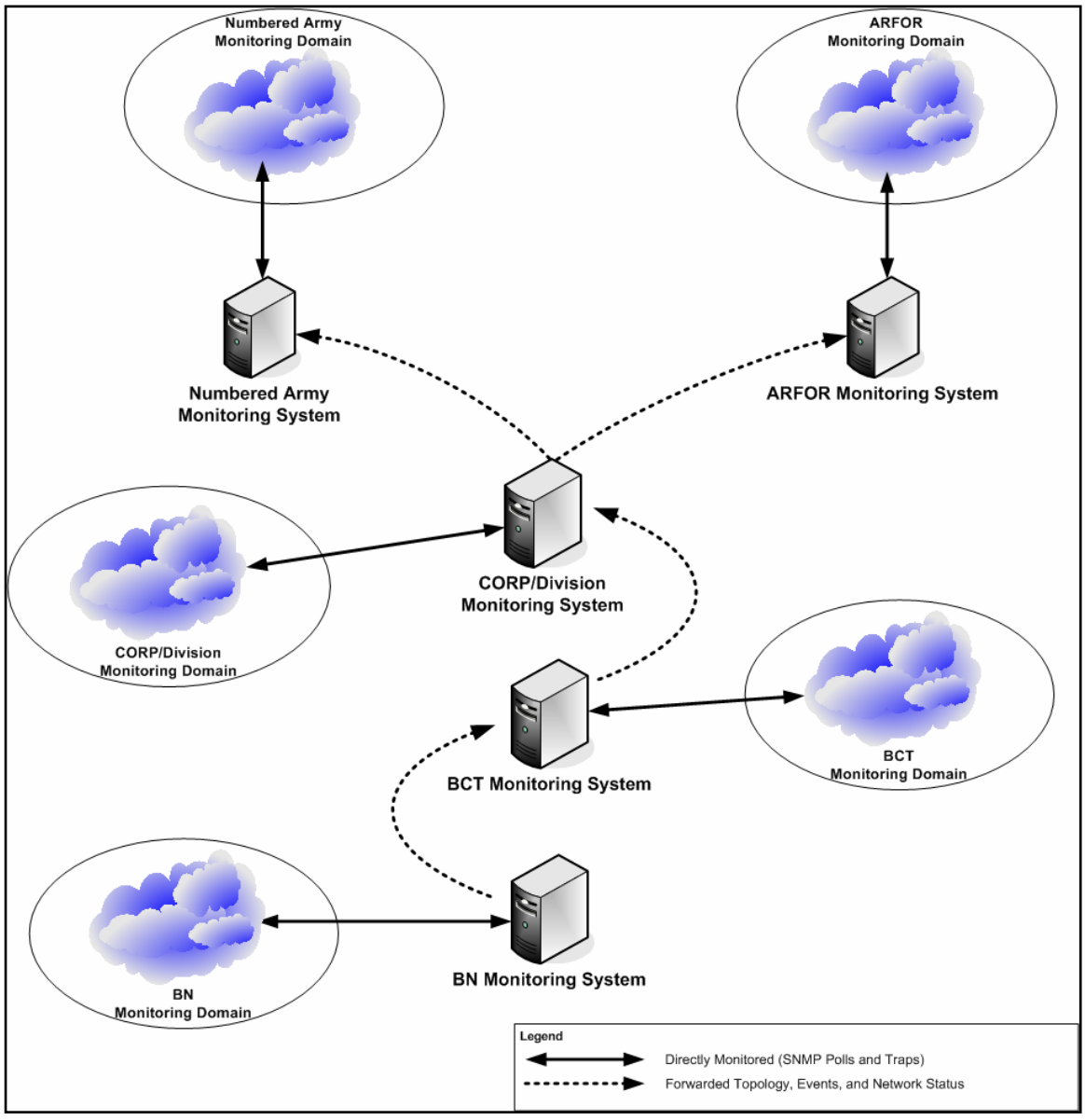

Figure 5-2. Distributed infrastructure monitoring example

5-106. The BCT will provide all monitoring information from its AOR and its subordinate battalion's AORs to the corps and division's NETOPS monitoring system. This information will consist of network topology and event and alarm data. This will provide the corps and division with a read-only view of the BCT's and battalion's infrastructure. The information received will facilitate troubleshooting and analysis activities.

5-107. Within the corps and division, infrastructure monitoring is performed by the G-6, signal company, supporting ITSB/ESB, TLT, and supporting signal organizations. The corps and division will use their NETOPS monitoring system to monitor, manage, and troubleshoot the network infrastructure within their AOR. The corps and division will provide all monitoring information from their AOR and subordinate BCT's, and battalion's AORs to the ARFOR NETOPS monitoring system. This information will consist of network topology and event and alarm data that will provide the ARFOR with a read-only view of the corps', division's, BCT's, and battalion's infrastructure, thereby facilitating troubleshooting and analysis activities. The corps and division is also responsible for making consolidated AOR monitoring information accessible to subordinate assets for SA and troubleshooting purposes.

5-108. The numbered Army will use its NETOPS monitoring system to monitor, manage, and troubleshoot the network infrastructure within its AOR. In addition to supporting these activities, the numbered Army's NETOPS monitoring system will be used to assist in the troubleshooting activities within the combat AOR, as required (see below for incident and problem management). The numbered Army is also responsible for making consolidated Army theater monitoring information accessible to the CCDR, A-GNOSC, and tactical Army assets within the theater for SA and troubleshooting purposes.

Infrastructure Monitoring/Management Joint Implications

5-109. The ARFOR is responsible for the management of the NETOPS capabilities and infrastructure within its AOR. Within the ARFOR, infrastructure monitoring and management activities will be performed by the G-6, supporting ITSB/ESB, TNT, and supporting signal organizations. The ARFOR conducts this mission through the monitoring and management activities conducted by subordinate ITSB/ESBs, corps, divisions, BCTs, and any other monitoring domains within the Army combat AOR. The ARFOR will provide all monitoring and management information from the Army combat AOR to the numbered Army's NETOPS monitoring system, which will consist of network topology and event and alarm data from its subordinate organizations. The ARFOR is also responsible for making consolidated AOR monitoring and management information accessible to subordinate assets for SA and troubleshooting purposes. For more information regarding troubleshooting and trouble ticketing, see Appendix C.

5-110. According to joint guidance, the CJTF and JFLCC will direct NETOPS monitoring and management within their respective AORs. Army assets supporting joint commands will perform monitoring and management functions according to the processes listed above, unless these processes conflict with joint guidance. Any conflict between joint guidance and army requirements will be adjudicated by the Army G-6.

NETOPS Operational Control and Management

5-111. There are two distinct and complementary NETOPS activities discussed in this section: operational control and operational management. Operational control of a NETOPS system, capability, or component involves the day-to-day activities involved in keeping the system, capability, or component running. Some of these activities include providing power, environmental controls, cleaning, preventative maintenance, installation, deinstallation, physical inventory, and touch labor. Operational management activities include configuration, reconfiguration, monitoring, patching, and upgrading. Some of the devices include computing platforms, routers, switches, multiplexers, uninterruptible power sources, encryption devices, and IDSs.

5-112. Operational control and management responsibilities are determined by global policy and the network topology. Even though the transmission system is relatively flat, the interconnection of IP networks is organized in a hierarchy. The demarcation points between the tiers (refer to Appendix I for tier detailed information) of the hierarchy in conjunction with tactical unit boundaries are natural borders for OPCON and management. Operational control of NETOPS capabilities, systems, and components is the responsibility of the unit that has physical control of the item. Operational management of NETOPS capabilities, systems, and components falls into the following three categories:

- **Unit managed component systems**. The operational management of a component or system, not capable of being remotely managed, falls to the echelon that physically controls the component

or system. One example of such a system is the squad level radio. Although all components and systems require a certain amount of touch labor, many components or systems may be under the operational management of a remote echelon. A limited set of touch labor functions such as installation, disaster recovery, troubleshooting, and deinstallation may be performed by local personnel under the direction of an echelon with remote operational management responsibility.

- **Echelons above corps and division capabilities**. Some systems are managed and operated as a capability by echelons above the corps or division. These systems may be more efficiently provisioned from a higher echelon, or may require centralized management. These systems are designed and implemented to provide flexible capabilities and do not require frequent reconfiguration in response to tactical mission requirements. Some examples of echelons above corps capabilities include the Army DNS system and the joint router network. Operational management of these systems resides at the echelon which provides the supporting capability.
- **Echelon above brigade managed systems**. The remaining NETOPS capabilities, systems, or components are both remotely manageable and require a distributed management structure to ensure that configurations are dynamically aligned with command requirements. Operational management of these systems within the corps or division and below falls to the tactical echelon directly above the brigade. In most cases, this will be a division. In some scenarios, the echelon above brigade may be a corps, numbered Army, ARFOR, or a joint command. The corps and division are augmented by the TIC to perform these functions. The ARFOR or joint command is augmented by a TNT to perform the same functions. Operational management of these types of systems within the echelons above corps generally falls to the supported echelons above corps command. For example, all remotely manageable systems within an ITSB/ESB-supported ARFOR TOC, as well as the ITSB/ESB itself, fall under the operational management of the ARFOR command. The only exception to this rule is when the SB(T) itself is operationally controlled to echelons above corps command in order to provide an additional span of control for echelons above corps networks. When this occurs, the signal brigade (theater) assumes operational management of the supported command's ITSB/ESB systems. Some examples of echelon above brigade managed systems could be called managers, VOIP gateways, private branch exchanges, routers, firewalls, collaboration tools, and unit directory services.

Note. Any echelon with operational management may delegate this responsibility to subordinate echelons or organizations as needed.

Operational Control and Management Echelons and Organizations

5-113. Operational control and management are executed at all echelons. The component types in the NETOPS infrastructure are the same regardless of whether they are located in a numbered Army, corps, division, BCT, or battalion. These include, but are not limited to, routers, data switches, voice switches, private branch exchanges, multiplexers, satellite terminals, line of sight transmission equipment, and computing platforms. Location and ownership of a NETOPS capability, system, or component will often affect which echelon or organization has operational control. For example, a unit-managed radio within the corps or division signal company is operated and managed by the corps or division, whereas the same type of radio within a brigade signal company is managed by the brigade.

5-114. The numbered Army is responsible for the operation and management of capabilities, systems, and components for its entire AOR. The TNOSC OPCON to the numbered Army executes OPCON and management in support of the G-6 and SC(T). In addition to managing and operating capabilities, systems, and components to conduct business on its portion of the NETOPS infrastructure, it has the responsibility to operate and manage support services for the tactical AOR. Some of these capabilities include Army DNS, IDSs, and Tier-1 routing domains. See Appendix I paragraph I-41 for an explanation of Tier 0, Tier 1, and Tier 2.

5-115. The deployment of an IDS to an organization is a good example to illustrate the operation and management responsibilities of several devices within multiple organizations. For this example, assume that

a pre-configured IDS is shipped to an organization. The receiving organization installs the IDS and connects it to the IP network (operational activity). A precoordinated IP address was configured on the IDS, which is immediately active on the LAN. Some of the activities that the local organization may have to perform to provide end-to-end connectivity is to create a reservation in their Dynamic Host Configuration Protocol (DHCP) server (manage DHCP activity) and reconfigure the local firewall(s) to permit the protocols and IP address of the IDS (manage firewall activity). The TNOSC will have to reconfigure their firewall(s) and reconfigure their IDS management station to complete the deployment. There are a number of operational and management activities on several devices in the respective organizations to successfully deploy the IDS capability. The receiving organization could be a corps, division, brigade, BCT, or a battalion.

Operational Control and Management Joint Implications

5-116. The ARFOR delegates responsibility for the operation and management of capabilities, systems, or components within its AOR to the corps, division, and directly reporting BCTs as appropriate.

5-117. The numbered Army will perform OPCON and management of Army Service components operationally controlled to the JTF in support of the joint mission. The TNOSC OPCON to the numbered Army executes OPCON and management in support of the G-6 and SC(T). The CJTF and JFLCC will orchestrate and coordinate the operation and management of NETOPS capabilities, systems, and components.

NETOPS NETWORK DEFENSE MANAGEMENT

5-118. The management of security is integral to and included in each of the NETOPS activities described in this chapter. This section is focused on security-specific activities that support the other NETOPS activities described throughout the chapter.

5-119. NETOPS security management includes the defensive components of IO that serve to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. The provisioning of many IA capabilities is implemented as Army enterprise capabilities. For example, Microsoft Windows AD is expected to provide enterprise-wide identification and authentication for Windows platforms.

5-120. Fundamental to the provisioning of the defensive components of NETOPS is the concept of DID. DID identifies three network-accessible areas that require defensive measures:

- **Perimeter** defense includes protections for both public and extranet access. Extranet access includes those ports and protocols that are external to and specifically identified by the tactical unit. Extranet A private network that uses IPs and the public telecommunications system to securely share information among selected external users. An Extranet requires the use of firewalls, authentication, encryption, and VPNs that tunnel through the public network (see AR 25-2).
- **Enclaves** are usually contiguous networks that support a specific geographical location, organization, or unit.
- **Hosts** are the final layer of defense. Protection at this layer consists of host-based configuration parameters and host-based intrusion detection and prevention software.

5-121. To support these defensive components, security information management tools are employed to support security event collection, data reduction, and correlation.

Security Management Echelons and Organizations

5-122. NETOPS security management is centralized to the greatest extent possible. Centralization ensures consistency and minimizes the number of personnel with the highly specialized skills needed to perform NETOPS security analysis. For NETOPS security management to be effective, it must be performed in near real time. This includes the ability for near real-time 24 hours a day, seven days a week operational control

and management of NETOPS security components and sensors. Security information management tools may be employed by the TNOSC in support of tactical organizations to efficiently aggregate and analyze NETOPS security event information.

5-123. Centralized management of NETOPS security perimeter protection components and sensors is performed by the TNOSCs within each theater. The operational tempo may require support from the TNOSC deployment support division to ensure that the commander's needs are met with respect to NETOPS security for deployed forces.

5-124. The TNOSC also manages NETOPS security enclave protection components and sensors. At the discretion of the chain of command, this responsibility may be delegated to the corps, division, or BCT level organizations. Enclave protection will also be performed at the corps, division, or BCT level if connectivity to the TNOSC is interrupted.

5-125. Local commanders at all levels have responsibility for host protection. ITSB/ESB and signal company personnel will provide assistance to local commanders as requested or directed.

Security Management Joint Implications

5-126. ARFOR, JFLCC, and CJTF NETOPS security management operations are governed by joint guidance. Army personnel supporting these organizations will operate within this guidance while also participating in Army security management procedures to the fullest possible extent.

5-127. Within the ARFOR, JFLCC, and CJTF, NETOPS security management operations are performed by the G-6, supporting ITSB/ESB, TNT, and the supporting signal organization. When a potential security incident is identified within or escalates to the ARFOR via a subordinate organization, its potential local impact is determined and it is escalated to both the appropriate NETOPS cell within the JFLCC or CJTF and the TNOSC. Appropriate responses or defensive measures are then directed via the chain of command.

INTERRELATIONSHIP OF NETOPS ACTIVITIES

5-128. It is important to note that the successful execution of the identified NETOPS activities requires a high degree of coordination and cooperation within and between responsible organizations at all echelons. The NETOPS activities described in this chapter are interrelated and dependent upon one another. For example, the incident and problem management activity relies upon the change management activity in order to implement corrective actions. This activity also relies on the infrastructure monitoring activity in order to detect anomalies. Appendix C provides more examples of the interrelationships between NETOPS activities and the organizations that carry them out. Figure 5-3 depicts the most common interrelationships that exist between the NETOPS activities.

NETWORK OPERATIONS EVALUATION CAPABILITIES

5-129. Within the operational environment, NETOPS capabilities must be evaluated to ensure that they are adequately supporting the Soldier. The evaluation activity is focused on the proactive maintenance of the health and protection of the NETOPS capabilities. Evaluation activities are grouped into two areas: IA compliance and NETOPS capacity and availability.

5-130. A NETOPS capability itself has requirements that must be met in order for the capability to operate normally. These requirements are characterized by key parameters that, when evaluated against a threshold, provide useful information about the health of the capability. For example, a key parameter of a T-1 circuit is the instantaneous transmission rate. When the instantaneous transmission rate exceeds 1.536 megabits per second (Mbps), the maximum transmission rate threshold has been exceeded and users of the transmission system can expect dropped packets and slow application performance (e.g., degraded availability).

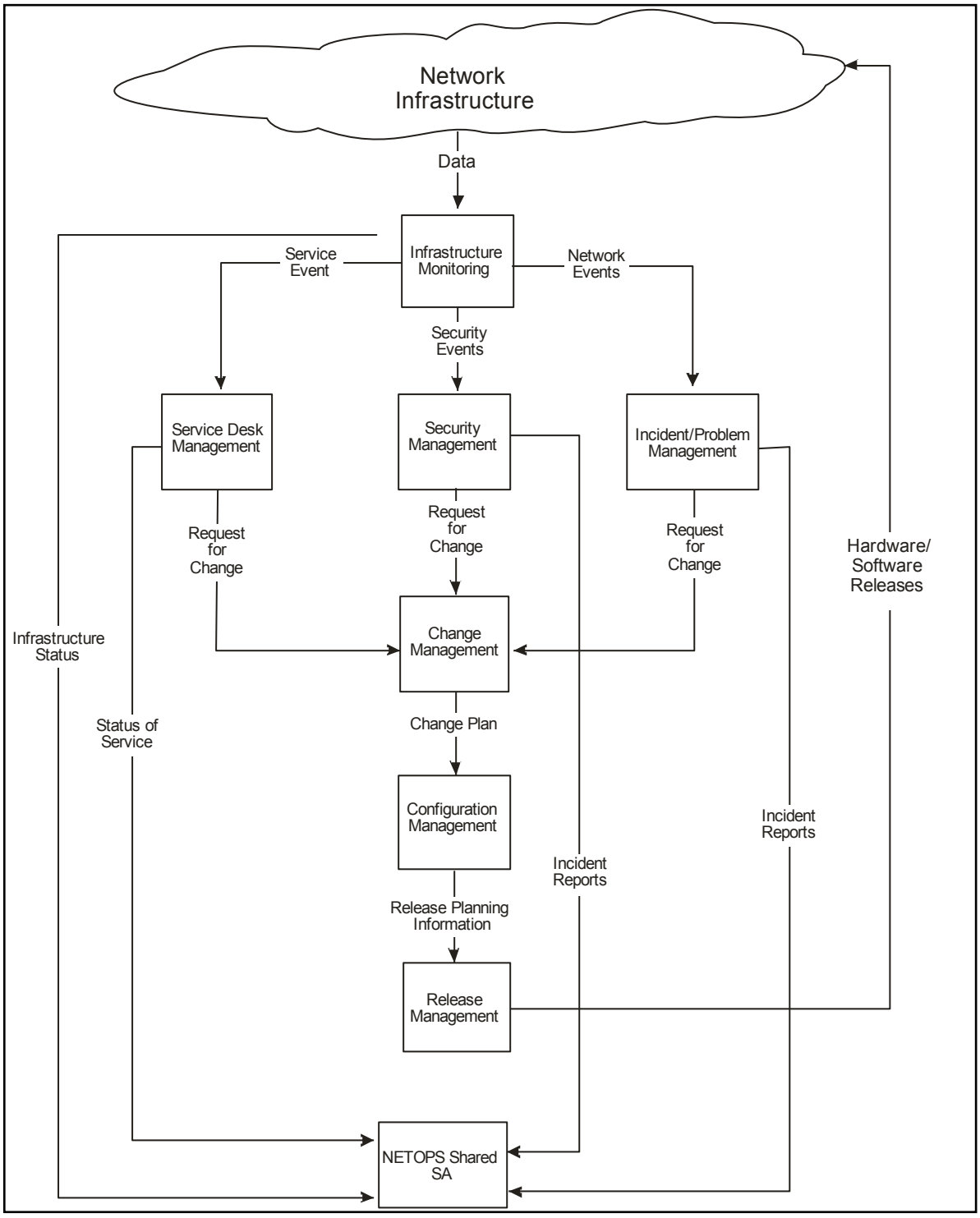

Figure 5-3. NETOPS operational activities process flowchart

5-131. NETOPS capability evaluation provides the information needed to identify degraded availability, capacity shortfalls, and IA compliance deficiencies. The result of the evaluation activities is information required for NETOPS capability planners, IA analysts, and engineers to apply remediation or isolation actions, reallocate resources, and identify upgrades to NETOPS capabilities supporting the Soldier.

5-132. The evaluation activities presented so far have focused on the health, maintenance, and protection of the NETOPS capabilities. The evaluation of trends over a long period of time provides information on the overall health of the NETOPS systems. The evaluation of trends illuminates training deficiencies and weaknesses in individual components or systems. It also provides valuable information to evaluate the effectiveness of doctrine, organization, training, materiel, leader education, personnel, and facilities.

IA COMPLIANCE

5-133. IA compliance relates to security management, which specifies the performance of vulnerability assessments. The evaluation of IA compliance, through CM, is the verification that the activities described in the Systems Maintenance Section of this chapter have been performed and any deficiencies have been identified. These assessments will be evaluated to ensure timely and adequate vulnerability remediation. The evaluation should be scheduled as part of the overall IA security plan.

5-134. A few of the NETOPS capabilities requiring IA compliance are represented by computing platforms, client applications, server applications, routers, and data switches that provide capabilities to the Soldier.

IA Compliance Echelons and Organizations

5-135. The A2TOC will provide IAVM messages for distribution to the theater teams, RCIOs, and DOIMs, and via AKO Knowledge Management bulk mail distribution. The RCIOs and DOIMs will ensure that corps, division(s), and BCTs comply with the IA updates. Compliance with IAVMSs and IA vulnerability bulletins must be reported in the Asset and Vulnerability Tracking Resource database. The updates are pushed to the organization with operational management for action. The corps and division G-6 has SA of echelons in the AOR and determines the appropriate time to apply the IA updates. In some instances, there are many baselines for a given NETOPS capability or there are too many to be supported by the numbered Army. In this situation, the tactical operations staff will have to modify, recreate, and test IA updates for distribution.

5-136. The corps/division G-6 has the responsibility to execute IA compliance IAW the commander's intent. The corps and division G-6 will use the appropriate resources (e.g., ITSB/ESB, signal company, corps and division sanctuary, TIC, and TNT) to accomplish this mission. The organization that executes IA compliance will be the organization with operational management of the system. The variety and complexity of the NETOPS capabilities requires specialized groups to operate and maintain the systems. For instance, the application of an IA package to a telecommunications component is best suited to the signal company or the ITSB/ESB. The organization that is chosen to perform the activity depends on the location of the component and which organization has OPCON. In another instance, the corps and division sanctuary would be the appropriate location to modify and apply a patch for a computing platform. Lastly, the organization with OPCON or management has the responsibility to provide compliance reports to the corps and division G-6 via the signal company or the corps and division sanctuary. The numbered Army will compile the compliance reports from the corps and division G-6.

IA Compliance Joint Implications

5-137. The ARFOR G-6 has the responsibility to execute IA compliance within its AOR IAW the ARFOR commander's intent. The ARFOR G-6 will use the appropriate resources (e.g., ITSB/ESBs, TIC, TNT, and subordinate G-6 or S-6) to accomplish this mission.

5-138. Upon request of the ARFOR, the numbered Army will evaluate IA compliance of Army Service components operationally controlled to the JTF in support of the CJTF. The CJTF and JFLCC will orchestrate and coordinate the evaluation of IA compliance of NETOPS capabilities, systems, and components.

NETOPS CAPACITY AND AVAILABILITY

5-139. There is a close correlation between NETOPS infrastructure capacity and availability of NETOPS capabilities. While the functions are different, the organizational responsibilities are identical. It should be noted that there is synchronization between the NETOPS capacity and availability and NETOPS infrastructure monitoring. Infrastructure monitoring is a short-term activity that will feed the long-term planning activity for such things as reallocation of resources with regards to IT capacity and availability.

5-140. The objectives of NETOPS infrastructure capacity evaluation are effective support to the Soldier and efficient use of NETOPS capabilities. The NETOPS capacity evaluation results in information to aid planners in forecasting capability degradation and making recommendations on capability reallocation and upgrades, and a host of other items to maintain the health and protection of the NETOPS infrastructure. Capacity evaluation encompasses all networking equipment, computing platforms, peripherals, and software. It involves monitoring the performance or operating level(s) of key parameters and comparing them against thresholds to forecast problems. The capacity evaluation activity provides critical, proactive information for infrastructure planners to better allocate resources and identify potential bottlenecks.

5-141. As previously mentioned, capability availability is closely tied to infrastructure capacity. The objective of availability evaluation seeks to ensure a sustained level of availability, reliability, and maintainability of NETOPS capabilities. The availability evaluation measures key parameters against thresholds to forecast service degradations. Availability evaluation encompasses all networking equipment, computing platforms, peripherals, and software. The results are used by NETOPS capability planners to improve the overall availability of the capabilities; ultimately resulting in a reduction of the frequency and duration of adverse incidents.

Capacity and Availability Echelons and Organizations

5-142. It is the primary responsibility of the corps, division, and ARFOR, with technical assistance from the numbered Army, to evaluate the capacity and availability of NETOPS capabilities. In addition, the mission, enemy, terrain and weather, troops and support available-time available may dictate that lower echelons, such as the BCT, perform this activity. The combined capacity and availability metrics and evaluations will then be reported to the corps or division.

5-143. The corps and division will monitor data under their control to evaluate capacity and availability metrics associated with NETOPS capabilities and enabling devices. The corps and division will also evaluate capacity and availability metrics from the BCT in order to form an assessment scoped to its AOR. The combined capacity and availability metrics and evaluations will then be reported to the numbered Army.

5-144. The numbered Army is responsible for evaluating the capacity and availability metrics associated with the NETOPS capabilities and enabling devices under their control as well as those provided by other service providers (e.g., DISA). The results of the evaluations are used to make capacity and availability improvements locally as well as to other NETOPS capability providers in support of the Soldier. The numbered Army will also evaluate its entire AOR based on capacity and availability metrics and evaluations collected from lower echelons. This investigation will help formulate an appropriate scoped assessment. This allows for the identification of issues that might not be seen when taking a narrower view from a lower echelon.

5-145. All capacity and availability improvement changes made to the NETOPS infrastructure at any echelon will be done through the established change management process. This ensures the proper level of coordination in keeping with the overarching goal of improved efficiency.

Capacity and Availability Joint Implications

5-146. The ARFOR will evaluate capacity and availability metrics associated with the NETOPS capabilities and enabling devices under its control. The ARFOR will also direct capacity and availability functions within the corps, division, BCTs, ITSB/ESBs, and any other subordinate signal organizations to

form an assessment scoped to its AOR. These metrics are then reported to the local numbered Army. Capacity and availability metrics are also evaluated and reported to its joint command as directed by joint policy.

NETWORK OPERATIONS TRAINING AND EXERCISE

5-147. As the capabilities and dependencies of the network evolve, the complexities of NETOPS and the management of the LWN and the GIG increase. NETOPS spans the entire enterprise and is no longer limited to just a local network, a small enclave, or a tactical battlefield, or the strategic environment. The Soldier is reliant on NETOPS capabilities continually being available. NETOPS capabilities are not just dependent upon the proper mix of equipment and processes. They demand a finely tuned, technically competent force that is continually being trained. Training and readiness responsibility is the driver for ensuring properly trained NETOPS forces. The Army provides a trained and ready force. It manages training from Army learning centers through the integrated command post exercise to support the CCDRs in exercising their Title 10 responsibilities.

5-148. Exercising these NETOPS activities has multiple impacts. First, it exposes many of the challenges that will be addressed by tools, technologies, and processes if the enterprise is to be fully leveraged as a war fighting platform. Second, it opens communications and exposes expertise and capabilities so that they may be leveraged across the enterprise. Only through exercising NETOPS activities will organizations learn the capabilities, challenges, and expertise that are required at each echelon to effectively provision NETOPS capabilities.

5-149. The activities Soldiers must perform in training are the same as when performed in an actual operational environment. The training environment should replicate as closely as possible the conditions, circumstances, and influences of an actual operational environment, except potentially in a physical location and that they may be augmented by simulation or stimulation. Detailed examples of NETOPS activities and their inter-dependant nature are provided in Appendix C.

TRAINING AND EXERCISE JOINT IMPLICATIONS

5-150. The Army must be ready to execute its mission as part of a joint force conducting joint operations. To accomplish this goal the Army must perform joint, interagency, intergovernmental, and multinational training. Some training must also be performed in the area of coalition network support.

5-151. To achieve joint operational interoperability, that being the joint tactics, techniques, and procedures as well as the processes associated with installation, operation, maintenance, and defense and NETOPS of LWN communications systems, joint operational interoperability must become an integral part of training requirements from Army learning centers to the integrated command post exercise. The joint operational interoperability training requirement should become a part of the training and readiness responsibility cycle for the CCDR. This will enhance the training of Army units on the interdependent activities and organizational relationships needed to perform joint NETOPS. It will also make it easier for Army units to integrate into the joint enterprise and to adhere to joint NETOPS standards and doctrine.

METHODS TO REDUCE FORWARD-DEPLOYED NETWORK OPERATIONS

5-152. The effort to migrate tactical NETOPS functions from the operational environment to a fixed-station location decreases the forward-deployed operational environment footprint, greatly facilitates coordination and data exchange between tactical units, and drastically increases the supportability of NETOPS functions. This can be approached via two distinct but complimentary methods: the migration of selected support services to the TNOSC and A-GNOSC, and the migration of tactical command functions to a unit-owned fixed station NETOPS cell.

METHOD 1: THE MIGRATION OF SELECTED SUPPORT SERVICES TO THE TNOSC AND THE A-GNOSC

5-153. As the physical network connectivity between the Soldier and sustaining base improves, it becomes advantageous to identify target opportunities for the extension of garrison and theater-based NETOPS capabilities to the Soldier. Consistent with Title 10 functions and responsibilities, these capabilities will be available to the Soldier wherever they deploy.

5-154. The evolution of tactical support services must be designed with the purpose of not impairing the flexibility or responsiveness of the ARFOR, corps, division, or BCT. Operational management responsibilities of the combat echelons are discussed in further detail within the NETOPS Operational Control and Management section.

5-155. For example, consider the AKO e-mail account and portal. The AKO e-mail address and portal are available wherever a Soldier or organization deploys. The organization does not have to worry about the operation and maintenance of this capability, and total cost of ownership is reduced. Additional examples of tactical support services are IAVA guidance, anti-virus updates, capacity and availability data collection and reports, and router configuration backups. The Soldier can access and manipulate these services by logging into an AKO or a TNOSC site.

5-156. It is essential that the numbered Army and theater Army stand up to this service paradigm so that opportunities to capitalize on economy of scale, standardization, and overall NETOPS value added are fully realized. This will help to meet the vision of a single integrated Army enterprise that is capable of projecting NETOPS capabilities in full support of the Soldier.

METHOD 2: THE MIGRATION OF TACTICAL COMMAND FUNCTIONS TO A UNIT-OWNED FIXED STATION NETOPS CELL

5-157. Many NETOPS functions require a distributed management structure which parallels the combat chain of command to ensure that activities are dynamically and quickly aligned with command guidance and user requirements. These functions are not candidates for migration to the TNOSC or A-GNOSC. Some examples of these functions are policy development, change management processing and approval, tactical engineering functions, tactical planning functions, and operational management of specific devices.

5-158. In order for these functions to take place at a fixed station location, it is necessary to stage a unit-controlled NETOPS cell within the fixed station. Robust lines of communication between the fixed station and the operational environment TOCs can then be utilized for intra-unit coordination and data exchange. The corps or division sanctuary serves this purpose for the corps and division. The TNT (rear) serves this purpose for the ARFOR, JFLCC, or the JTF.

5-159. Some NETOPS functions require direct physical interaction with equipment or personnel within the operational environment. Examples of these operational environment-linked NETOPS functions are touch labor troubleshooting, device installation, manual recovery and teardown, site reconnaissance, and physical interaction with unit subscribers or command personnel. These functions cannot be migrated to the corps or division sanctuary, the ARFOR, JFLCC, or the JTF TNT (rear). All other unit-based NETOPS functions for the corps, division, and above will be migrated to these locations.

5-160. There are few NETOPS tasks in the BCT and below that are not operational environment linked. For this reason, the BCT and below will not generally operate a unit controlled NETOPS cell within the fixed station. The BCT and below has the option of staging unit NETOPS services at the numbered Army-hosted fixed UHN. They can also place unit personnel at a corps or division sanctuary or a TNT (rear) in order to facilitate unit integration and provide remote NETOPS services from the fixed-station.

Appendix A

Active Directory

This appendix describes the AD concept for command and staff elements that deployable Army units will use to implement and operate AD in CONUS, OCONUS, and across all theaters of operations. This information is not meant to provide the technical procedures required to install, operate, and maintain networks in an AD environment. This document establishes that tactical unit guidance is provided by the US Army Signal Center and the US Army NETCOM/9th SC(A). They will provide the overall guidance for the standards, responsibilities, and processes necessary to migrate from the current IT environment to an AD based environment.

OVERVIEW

A-1. To meet the operational philosophy of training and working-as-you-fight, the deployable units should operate the same way in garrison as they would when they are deployed. This "deployed-in-garrison" concept helps to support modularity and achieve a "plug-&-play" functionality for the deployable units. Deployable force users will be able to leverage local DOIM or TNOSC expertise, as available. The users will increase and maintain automation proficiency by practicing the skills learned while providing service in garrison.

A-2. Introduction of AD into the Army will provide both a new capability plus satisfy the Army mandate for a technology replacement of the old NT 4.0 LAN operating system.

ACTIVE DIRECTORY OPERATIONAL FEATURES

A-3. The AD architecture and associated features introduce a more granular management capability with the introduction of structures such as forests, and organizational units. The enabling technology for all of these new structures is AD, which is the directory service for Windows 2003 server capabilities. AD implementation is both necessary and beneficial in that current disparate architectures and personnel responsibilities at each installation can be combined to form an Army Windows IT enterprise. Approved deployed forest information is in the approved Technical Authority 2006-006, 14 May 2007.

ENTERPRISE MANAGEMENT FEATURES

A-4. The enterprise management features include:

- **Extensible schema**—AD lets developers and administrators extend the directory schema and create new properties and objects. Using the directory as a data store, developers can create their own data structures for applications. Users on the network can publish important information in the directory so other users can easily locate the material.
- **Centralized management**—allows enterprise level management of Windows users, clients, and servers through a single consistent interface, reducing redundancy and maintenance costs.
- **Group policy**—allows administrators to define and control the policies governing groups of computers and users within their organization. Administrators can set group policy for any of the sites, domains, or organization unit in AD. Once the policy is set, the system maintains group policy without further intervention.
- **Global catalog**—provides a way to centrally maintain information about users and universal groups for access control. The information is managed by using one or more domain controllers

that contain subset attribute information for most entries in a Windows 2000 domain forest. These controllers also replicate domain schema, configuration, and partial user or other resource entries.

- **Automated software distribution**—provides the capabilities for administrators to automatically distribute applications to users based on their functional requirements.
- **AD service interfaces**—simplifies the development of directory enabled applications and the administration of distributed systems. Developers and administrators use this single set of interfaces to manage the resources in a direct support, regardless of the network environment that contains the resource.
- **Delegated administration**—provides administrators the ability to delegate a selected set of administrative privileges to appropriate individuals within the organization and specify the specific rights they have over different containers and objects in the directory.
- **Multi-master replication**—ensures changes made to any one domain controller will replicate to all the other direct currents in the same domain, and assures that the directory is available for changes 100 percent of the time.

Security

A-5. AD security features include:

- **Kerberos authentication**—provides fast, single sign-on to Windows-based resources and to other environments that support this protocol.
- **Transitive Domain Trust**—reduces the number of trust relationships to manage between the Windows domains.
- **PKI x.50**—ensures interoperability with and deployment of extranet and e-commerce applications.
- **Attribute-level security**—enforces object and attribute-level security for detailed control of access to information stored in the directory.
- **Spanning security groups—**permits central management of groups.
- **Lightweight Directory Access Protocol ACL support**—ensures interoperability for secure extranets and e-commerce applications.
- **Smart Card support**—allows logon via smart cards for strong authentication to sensitive resources.
- **Group policy—**allows administrators to define and control the security policies governing groups of computers and users within their organization and filter the effects by using membership in security groups.

ACTIVE DIRECTORY MULTI-FOREST AND OPERATIONAL CONSIDERATIONS

A-6. The current approved AD architecture represents a multi-forest approach that divides the Army enterprise into element permanent AD forests and allows for tactical forests.

A-7. Since the security boundary is at the forest level, a single forest approach produces a security vulnerability that is not acceptable. Single forest architecture would allow someone with access to the forest's domain controller or administrative rights in a domain to exceed their authority and obtain enterprise administrative rights. Objects stored in the AD represent all of the users, systems, and services within that forest. A person with these rights could destroy the validity of the data causing enterprise wide consequences. The global catalog contains a partial copy of every object in the AD forest. If the system that hosts AD for a forest is compromised, there is a risk of exposing a portion of the Army's infrastructure information. A larger forest makes more infrastructure information vulnerable at a central location. The multi-forest operational concept limits the consequences of an attack. The smaller the forest, the more readily problems associated with the global catalog can be discovered. The single forest has a limited ability

to compartmentalize. This circumstance presents an unacceptably high risk for secure information distributed into potentially hostile areas.

A-8. In addition to security considerations, scalability is an operational risk associated with a single forest deployment. The larger the forest size in terms of number of supported users and desktops, the larger the directory must be that supports the forest. Since the Army has in excess of 1,000,000 users, a single directory and the associated global catalog would be extremely large and would impose potentially excessive replication loads on available network bandwidth. The architecture of each forest will have a top level AD domain that forms a contiguous name space from the top level Army enterprise forest root domain; and a contiguously named management domain that is a placeholder domain to manage the enterprise administrator accounts and processes.

A-9. Organizations' geographic "regions" are included in a designated regional forest. Examples of regional forests are CONUS, Pacific, Korea, and Europe. In addition to the standard regional forests, some organizations require autonomy due to sensitive or specialized business practice or geographic region that does not adequately represent its mission support needs. For these cases, a "virtual region" and corresponding forest exists. Examples of organizations with their own "virtual region" include Army Medical Command, Corps of Engineers, and National Guard. Given the multiple forest configurations of AD, the A-GNOSC uses the CONUS-TNOSC operation and maintenance resources and capabilities to fulfill its Windows server or AD enterprise management role. The current list of forests are:

- North America forest: five child domains representing information management area regions.
- Europe forest: three child domains.
- Global catalog forest: three child domains.
- National Guard forest: four child domains.
- Pacific forest: three child domains.
- Southwest Asia forest: one child domain.
- Korea forest: one child domain.
- Corps of Engineers forest: three child domains.
- Education forest: to be determined.
- Enterprise Application forest: one child domain.
- Deployed forest information can be found in Technical Authority 2006-006, dated 14 May 2007.

ACTIVE DIRECTORY IMPLEMENTATION CONSIDERATIONS

A-10. When implementing AD the commander and staff must consider:

- Implementing, managing, and maintaining IP addressing as related to the DHCP.
- Name resolution as related to the DNS.
- Network security as related to overall security templates to include parameter security and CND oversight.
- Routing and remote access as related to remote access authentication protocols.
- Managing network architecture as related to connectivity to the Internet and troubleshooting network services.

A-11. A global catalog server is required to communicate between domains. There must also be a sufficient amount of automation materiel (hardware or software) for the deployable force. AD implementation needs an information system platform that meets or exceeds the performance requirements to run Microsoft Advanced Server 2000/2003 software domain controller, a DNS, DHCP server, and a global catalog server. The DNS may be co-hosted on the domain controller provided it does not adversely impact system performance.

FLEXIBLE SINGLE MASTER OPERATION

A-12. The enterprise flexible single master operation roles for each forest will be physically located on the domain controllers. Flexible single master operation roles will include the schema and domain naming masters. The root or management domain specific roles are—

- Primary domain controller emulator.
- Relative identifier master.
- Infrastructure master.

A-13. All domains in an AD forest share a single schema, configuration naming context, and a global catalog containing selected information about each object in the forest. The Army will maintain consistent schemas across all forest implementations. This is accomplished through strict adherence to published Army Enterprise Infrastructure (AEI) standards and tightly controlled change management through the CCB process. NETCOM chairs the AEI Tech CCB, which adjudicates modifications to the currently implemented AD schema in an operational environment.

Note. CCDR participation in and input to the AEI Tech CCB will aid future CCDR AD migration.

MANAGEMENT ROLES AND RESPONSIBILITIES

A-14. This section addresses the roles and responsibilities of Army organizations within the Windows server or AD enterprise. AD is a key component of any future enterprise-wide directory service. Therefore, the management and configuration control of AD implementations and maintenance requires strict central control and well-defined roles and responsibilities across the enterprise. The role of schema or enterprise administration is the responsibility of the local enterprise administrator, which delegates operation and maintenance responsibility to selected support and helpdesk personnel. NETCOM has been tasked by the CIO G-6 to establish technical guidance, procedures, and standards for AD implementation and operations. The current version of the AEI Directory Services Naming Conventions and Standards (NETC-EST-G-0306-009-STD), published by NETCOM Enterprise Systems Technology Activity is the authoritative document governing AD. This and other documents can be found at the following URL https://www.us.army.mil/suite/folder/626256. Figure A-1 shows the interface relationships by organizational level. Table A-1 shows the organizations by level with their associated operational roles.

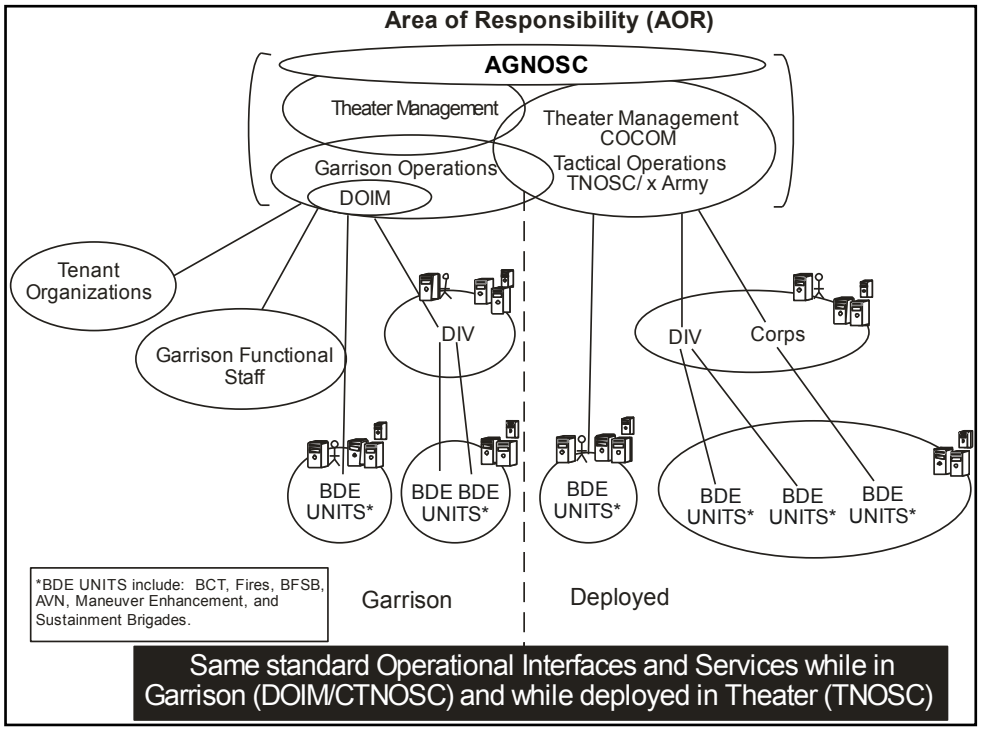

Figure A-1. AD operational interfaces by NETOPS organizational level

Table A-1. AD operational concepts by NETOPS organizational level

NETOPS Level		
GARRISON	***DEPLOYED***	***AD Operational Roles***
Unit Level ***Corp, Division, and Brigade Unit***		Has specific responsibilities for: • Exchange e-mail. • Web hosting and collaboration (information dissemination management-tactical [IDM-T]). • AD and user account management. • Patch management to defend the tactical network. • File, print, and store.
Installation and numbered Army level		The site or installation will be a top-level organizational unit. Has specific responsibilities for: • Collaboration services (Defense Collaboration Tool Suite and information warfare support). • Record messaging services (Defense Message System and Automated Message Handling System). • Perimeter security; CND oversight. • Trouble ticketing services. • Global address list synchronization. • Level 2 and 3 technical support and operational CM. Provides NETOPS shared SA data to respective TNOSC.
DOIM	***Major Subordinate Command***	
Theater Level		Manages and administers AD forest and domains for the respective theaters; delegates top-level organizational units' administrative roles to ensure efficient, effective distributed operations for lower level organizations.
DOIM	***TNOSCs***	Provides expertise to support the expanded enterprise operation and maintenance of critical domain and theater level AD equipment Monitors network common relevant operational picture (NETOPS shared SA) for installations in region.
Global Level ***NETCOM (A-GNOSC)***		Provides all Army users enterprise-wide visibility and access to "yellow and white" pages. Establishes technical guidance, procedures, and standards for AD support. Has specific responsibilities for: • SA. • Domain naming service master. • Circuit management. Provides top level configuration control through AEI Tech CCB.

KEY AD MANAGEMENT ROLES IN THE MULTI-FOREST ARCHITECTURE

A-15. The multi-forest architecture provides the foundation for the operation and maintenance support of the Army AD community. AD provides the capability, at the enterprise level, to support the mission to manage, operate, maintain, monitor, and defend the AEI. The master forest (ds.army.mil for NIPRNET and

ds.army.smil.mil for SIPRNET) provides the framework for Army enterprise management using Microsoft's Windows 2003 AD services across all approved forests. The key aspects of the AD environment requiring central control are—

- Schema and naming standards throughout the multiple forests.
- Administration of the domain controllers precludes the delegation of specific privileges below the central management organization.
- AD and Windows 2000/2003 server administration capabilities do not preclude the delegation of specific privileges required by local support staff. This delegation of responsibilities may be handled via third-party software tools.
- Execution of administrative roles.
- Forest level administration of the AD forest includes responsibilities related to managing the AD schema and those tasks requiring enterprise administrator privileges.
- Domain level administration of the AD domain includes responsibilities of domain management and maintenance of the domains within the forest, to include all tasks requiring domain administrator privileges.
- Administration of the top-level organization unit includes responsibilities of organization unit management and maintenance to include user, group, resource, and data administration.

UNIT LEVEL

A-16. Units may operate and maintain specialized IT resources such as specialized software or hardware devices required to perform the unit's mission. These resources remain the operation and maintenance responsibility of the unit. These organizations use standard Army support to the greatest extent possible, thus minimizing differences.

Corps, Division, and Brigade Mission-Critical Services

A-17. Corps, division, and brigade mission-critical services include:

- Organizational messaging (Defense Message System).
- Exchange e-mail.
- Web hosting or collaboration (IDM-T).
- Managing user accounts within their unit based on the AD policies and administrative capabilities.
- Patch management to defend their network.
- Hosting and maintaining local print servers, local file servers, and local storage.
- DNS management.
- AD replication; DHCP authorization.
- Trust management.
- Local exchange message tracking and troubleshooting.
- Perimeter security and CND oversight.
- Managing and creating domain local groups.
- Managing NETOPS.
- Trouble ticketing and helpdesk services.

Additional Corps, Division, and Brigade Required Services

A-18. Additional corps, division, and brigade required services include:

- Providing group policy object policy administration to include domain and domain controller polices.
- Providing level 2/3 technical support and operational CM.

- Maintaining the approved configuration of core AD equipment on the installation or region as directed by its TNOSC related to the initialization or termination of operations and to the establishment or maintenance of configuration.
- Populating and managing organization units provided, and delegating authority for subordinate level organization units.
- Applying security necessary to prevent unauthorized individuals any physical access to enterprise resources geographically located at the installation.
- Notifying appropriate higher command of physical security compromised of any system.
- Executing global catalog server roles.
- Executing schema master role for the unit forest.
- Executing domain naming master role for the forest.

INSTALLATION AND NUMBERED ARMY LEVEL

A-19. Organizations at the installation or numbered Army level may operate and maintain specialized IT resources such as specialized software or hardware devices required to perform their mission as well as their subordinate unit's missions. These organizations include TNOSC, DOIM, and major subordinate commands (e.g., CCDRs). These resources remain the operation and maintenance responsibility of the unit, and the organization's commander will act as the designated approval authority (DAA). These organizations use standard Army support to the greatest extent possible to minimize differences. Critical tasks include all the tasks required at the unit level as well as the tasks requiring AD enterprise, domain administration, and exchange rights. These tasks include:

- DNS CM.
- Collaboration services (Defense Collaboration Tool Suite and information warfare support).
- AD replication; DHCP authorization.
- Group policy object policy administration to include domain and domain controller polices.
- Trust management.
- Exchange installation and message tracking and troubleshooting to include:
    - Trouble ticketing services.
    - Record messaging services (Defense Message System and Automated Message Handling System).
- Enabling global address list synchronization.
- Perimeter security; CND oversight.
- Level 2/3 technical support/operational CM.

DOIM AND MAJOR SUPPORT COMMANDS

A-20. The DOIM and the major subordinate commands in the US Army theaters have two basic functions: one of operational support and one of administration and management. These organizations provide infrastructure IT services to all Army users on the installation, consistent with the concept established by the NETOPS CONOPS. In addition, they provide access to IT services based on support agreements with other non-Army organizations and activities. From a Windows server or AD perspective, DOIM and major subordinate command activities include:

- Conducting Windows server and AD implementation, and coordinating the necessary implementation planning actions with NETCOM and its TNOSC.
- Hosting and maintaining local print servers, local file servers, and local Windows servers for legacy systems interaction.
- Ensuring that noncritical member servers provided by the installation meet the minimum server requirements to join the enterprise.
- Providing troubleshooting support for core AD servers in support of the TNOSC operation and maintenance responsibilities.

- Performing necessary hands-on maintenance of AD assets ICW its TNOSC.
- Managing user accounts within their installation or region based on the AD policies and administrative capabilities.
- Maintaining the approved configuration of core AD equipment on the installation or region as directed by its TNOSC related to the initialization or termination of operations and to the establishment or maintenance of configuration.
- Managing and creating domain local groups.
- Populating and managing top-level organization units provided as part of the installation resources and delegation authority for subordinate level organization units.
- Validating and forwarding, through the RCIO, all configuration change requests from local organizations.
- Maintaining installation member servers and applications.
- Applying security necessary to prevent unauthorized individuals any physical access to enterprise resources geographically located at the installation.
- Notifying the TNOSC of physical security compromised of any system.

THEATER LEVEL

A-21. At each theater level, the TNOSC has the key management role for the Windows server and AD operations within that theater. In general, these roles are the forest and domain administrative related roles as delegated by the A-GNOSC.

TNOSC

A-22. The TNOSC is the highest-level organization with IT operations responsibilities. They interact with the RCIOs and with the A-GNOSC. Within a given theater of operation, the TNOSC has the responsibility for IT assets that span its theater. It is responsible for ensuring that IT assets operate correctly, and for creating policy on a theater-by-theater basis. The TNOSC currently manages the public side of the demilitarized zone. Note that the demilitarized zone currently starts at the installation Army DISN router program. The TNOSC supplies technical support (e.g., tool sets to ensure the local health of AD) to the installations. The TNOSC proactively monitors all systems within the child domains. Each TNOSC is responsible for the performance management to support AD operations in theater. TNOSC performs the appropriate monitoring for those systems within their child domains. They use the information to affect root level configuration change request through the A-GNOSC to the AEI technical CCB.

A-23. The TNOSC is responsible for ensuring standard configuration, CONOPS, and centralized management of domain controllers within the Windows server or AD enterprise. It ensures the systems located in these domains are capable of providing those services detailed in the Army enterprise, AD architecture, and any subsequent AEI technical CCB additions. The TNOSC maintains the necessary system configuration, conducts theater level Configuration Control Review Board, and implements system changes authorized by the AEI technical CCB. The TNOSC ensures proper configuration of external devices and provides the backup and recovery processes relative to child domains. Under the AD enterprise concept, the TNOSC's responsibilities will expand and include the administrative management of the domain for the theater's respective AD. These responsibilities include:

- Operating and maintaining the domain controllers for all domains and the critical member servers in the theater.
- Maintaining and disseminating enterprise management and directory management tools.
- Hosting and maintaining:
    - DNS server for the theater's domains (DNS server is a secondary for the root zone).
    - Infrastructure master role for theater respective domains.
    - Primary domain controller emulator role for theater domains.

A-24. TNOSC executes security related guidance from the A-GNOSC by implementing security programs, procedures, policies, and IAVA patches as directed. It is imperative that the TNOSC take all actions to protect its domain level systems from compromise. TNOSC provides a level of physical security ensuring that only authorized individuals have access to their child level domains. TNOSC will notify the appropriate organizations if systems are compromised within their domains and will provide the organizations with all the information relative to the compromise. TNOSC will implement best security practices by controlling accounts relative to administrative functions within respective domains.

A-25. The respective TNOSC also has regional level responsibilities for the domain hub domain controllers that are established in a region. Each TNOSC will have the administrative rights for the child domains affected by these domain controllers for that region. The NETCOM domain design document provides the technical guidelines for the functions of these domain controllers. The respective TNOSC has site level responsibilities for the domain replicas on each site. The TNOSC has the administrative rights for the top level organization units for the site. The NETCOM domain design document provides the technical guidelines for the functions of these domain controllers.

REGIONAL CHIEF INFORMATION OFFICER

A-26. The RCIO acts as the CIO for an assigned region. The RCIO ensures all personnel operating on an Army installation are provided the IT resources they require in a manner that is consistent with policies, regulations, and other guidelines developed in or by the RCIOs management chain. The RCIO provides administrative and managerial IT support to any DOIM located within its regional director geographic region.

GLOBAL MANAGEMENT ROLES

A-27. This section addresses the role of those global level organizations that affect Windows server and AD operations. Refer to the Army Knowledge Management NETOPS CONOPS for a complete description from a NETOPS perspective of all organizations for the global level.

ARMY GLOBAL NETWORK OPERATIONS AND SECURITY CENTER

A-28. The A-GNOSC's prime responsibility for Windows server and AD operations is to establish and exercise strict control over the AD forests at all levels within the enterprise. The proactive centralized monitoring of enterprise systems within the Army AD environment provides organizations responsible for those assets the valuable information necessary to achieve a stable and productive enterprise environment. The A-GNOSC provides operational and management policy input to NETCOM. The A-GNOSC delegates AD administrative roles by:

- Assigning the responsibilities for schema and enterprise administration at the forest level to the appropriate TNOSC.
- Assigning operating responsibilities for cross-forest meta-directory services to the appropriate TNOSC.
- Assigning responsibilities for administration at the top-level organization unit and delegation of administrative authority to the installation DOIM or major subordinate command organization unit administrators.
- Assigning responsibility for administration at the second-level organization unit or below by the major subordinate command or DOIM to other lower-level organizations.

A-29. At present, the A-GNOSC uses the CONUS-TNOSC capabilities and resources to conduct its AD enterprise management functions. The A-GNOSC has the following roles and responsibilities relative to the Army AD enterprise:

- Delegates, to the TNOSC, the responsibility to perform the appropriate monitoring for all systems within TNSOCs respective domains. The scope of this responsibility includes hardware, operating systems, services (to include the Army AD), networking services, third party tools, Windows 2003 policies, sites, organizational units, and enterprise accounts.

- Delegates to the TNOSC operation and maintenance support actions, to include:
    - Management of the enterprise management and directory tools in the management and services domains of the master forest.
    - Global catalog server at the root level.
    - Schema master role for the forest.
    - Domain naming master role for the forest.
    - CM support responsibilities.
- Ensures maintenance of a standard system baseline, and overall administration of systems located within all approved forests supporting the actions of the AEI technical CCB. The AEI technical CCB has overall responsibility for CM of the Army IT enterprise.
- Establishes processes with the respective TNOSCs for a theater level CCB to implement processes for the following call manager actions:
    - Implement CCB approved system changes for the root domains.
    - Ensure that approved configuration changes are propagated to child domains within the Army AD domain structure.
    - Maintain the system configuration for the hardware, software, and applications necessary for the CONOPS of systems in the root level domains based on standard server configuration document.
    - Ensure proper configuration of external peripheral devices and provide the management of the backup and recovery systems within the root domain.
    - Ensure consistency across the enterprise for AD supporting tools sets via requirements developed ICW NETCOM product engineers.
- Participate in an advisory role to the AEI technical CCB to provide operational expertise.

A-30. A-GNOSC identifies, tracks, and manages all security areas relative to enterprise servers for all forests. A-GNOSC directs the respective TNOSC implementation of security programs, procedures, policies, and IAVA patches. A-GNOSC administers control over accounts relative to administrative functions within the root domains, and uses whatever means necessary and reasonable to ensure security of the root systems. A-GNOSC is responsible for notifying the appropriate organizations if systems within the root level are compromised. They also provide that organization with all the information relative to that compromise.

A-31. The greatest level of protection must be exercised in guarding the Army AD data. Given the existence of host-based IDS, the A-GNOSC directs the respective TNOSC to configure the software in such a way as to maximize the efficiency of the software while balancing system performance. Security management duties include:

- Managing the settings for encryption level between root and child-level domains.
- Coordinating with the TNOSC in order to implement encryption levels.
- Establishing the accounts and access permissions to the file systems located within the root domains.
- Ensuring that user and administrative accounts within the root domain have proper password security.
- Ensuring user and administrative accounts have not been compromised.

NETWORK ENTERPRISE TECHNOLOGY COMMAND

A-32. NETCOM was designated as the Army's authority to operate (ATO) and manage the enterprise level infrastructure. NETCOM is also in charge of implementing Army IT operational and management policies. Through operational review and coordination, NETCOM agencies establish standards and evaluate devices that impact upon the Army enterprise level infrastructure.

A-33. NETCOM delegates the management of Windows server and AD operational services by assigning administrative roles to the Army organizations. From the Windows server or AD perspective, NETCOM responsibilities are:

- Integrating, operating, and maintaining the Army's protected (public) and AD (private) DNS.
- Providing processing platform management and administration of all AD enterprise level servers.
- Managing the Windows server and AD top-level architecture (this includes domain management of all consolidated Windows 2003/2000 domains and domain controllers).
- Managing the root and services domain (ds.army.mil) for the enterprise.
- Providing support for organizational unit managers.
- Providing policy and technical guidance to installations or sites for migration to the Windows server and AD.
- Integrating directory services.
- Integrating AD with TNOSC COOP.
- Integrating Windows server and AD developed backup and restore technology.
- Operating, managing, and maintaining Windows server and AD root and regional footprints.
- Managing COOP and backup and restore technology for Windows server and AD systems.
- Expanding security monitoring to support enterprise Windows server or AD servers.
- Testing and applying all security patches and validating IAVA compliance for all AD and consolidated servers.
- Assisting with the installation DOIM as necessary during the execution of the approved plan.
- Validating compliance IAW AEI technical CCB.
- Accommodating issues that prevented routine migration of installation users or organizations.

ARMY CHIEF INFORMATION OFFICER G-6

A-34. The CIO G-6 is responsible to the secretary of the Army and responsive to the chief of staff of the Army for all information management area activities of the Department of the Army. The information management area includes automation, communications, records management, publications and printing, visual information disciplines, and library activities throughout the Army theater and strategic (tactical and sustaining base) environments. From a Windows server or AD perspective, the CIO G-6 activities include:

- Providing high level (global) Windows server or AD policies.
- Establishing high level (global) Windows server or AD operating rules and guidelines.

TACTICAL INTERNET NAMING CONVENTIONS

A-35. The naming standards described in this document apply to all Army networks of all classifications, strategic and tactical. This appendix covers the specifics that apply to all tactical and deployable Army units (active and reserve) and is intended to be used in conjunction with the entire Naming Convention document, making it interoperable with the naming convention of the DISN and the tactical naming conventions of other tactical forces. It is not intended to be used as a stand alone document. This appendix incorporates data networks at theater, corps, division, BCT, combat aviation brigades, fires brigades, combat support brigades, sustainment brigades, battlefield surveillance brigades, and battalion/small command posts. This naming convention applies to both tactical SIPRNET and tactical NIPRNET addressing with the difference in domains of ".army.smil.mil" for SIPRNET and ".army.mil" for NIPRNET.

Note. This guidance document is based on current policies and procedures at the time it was written. Any changes in policy or guidance could impact this guidance and will be reviewed as needed.

A-36. NETCOM and the US Army Signal Center agree to support the following SECRET Internet Protocol Router (SIPR)/Non-Secure Internet Protocol Router (NIPR) DNS structure for autonomous units. Autonomous units are defined as any unit that satisfies the Joint Expeditionary Mindset (Task Force Modularity) and can be deployed without regard to any habitual relationship or task organization, CONUS or otherwise. Notable examples include the reorganized BCT or other brigade unit, division, and corps and/or theater.

A-37. The autonomous unit maintains its SIPRNET/NIPRNET AD forest and only one AD domain. If the autonomous unit desires additional domains, they must be approved by NETCOM ICW the US Army Signal Center.

ACTIVE COMPONENT TACTICAL/DEPLOYABLE AD FORESTS NAMES

A-38. Tables A-2 through A-4 are the standardized names to be used upon approval of AD tactical/deployable forests. Inclusion in this list does not constitute an approval for implementation. All forests must be approved by the CIO/G-6 prior to implementation based on current policies and procedures. No deviations are authorized. Any additions to this list must be requested from the proponent for this publication. Current information (Army guidance) is in Appendix M of the AEI directory services naming conventions and standards document. For the most current Appendix M please click the URL listed below. https://www.us.army.mil/suite/collaboration/folder_V.do?foid=807867

DOMAIN NAME

A-39. Each tactical/deployable forest will initially have only one AD domain. Its name has been assigned according to Tables A-2, A-3, and A-4 below. In the event that additional domains are required, requests must be coordinated, through the unit's parent G-6/S-6, with the Global Database Manager at the US Army Signal Center (Concepts, Requirements and Doctrine Division, Material Requirements Branch), DSN: 780-6920) for concurrence; and then must receive approval from NETCOM.

Note. The ".DS" appears only in the root domain name; the nameserver record pointing to the tactical DNS servers IP will be for public presence namespace and is the same as the existing namespace but without the DS. The unit does not include the ".DS" in its request for a nameserver record (with its DNS IP) to be added. Example: A server is installed using the DNS namespace 3BCT82AB.ds.army.mil or 3BCT82AB.ds.army.smil.mil. The nameserver IP is registered with 3BCT82AB.army.mil or 3BCT82AB.army.smil.mil for external resolution. If a system on the internal network needs to be publicly accessible then an alias record would be created in the 3BCT82AB nameserver pointing to the internal machine. This ensures that only authorized systems are resolved from outside of the unit's network.

Table A-2. Forest names, domain names, and exchange organization names of active component tactical deployable units

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
Corps			
ICorps	ICORPS.DS.ARMY.MIL	ICORPS.DS.ARMY.SMIL.MIL	ICORPS
IIICorps	IIICORPS.DS.ARMY.MIL	IIICORPS.DS.ARMY.SMIL.MIL	IIICORPS
VCorps	VCORPS.DS.ARMY.MIL	VCORPS.DS.ARMY.SMIL.MIL	VCORPS
XVIIICorps	XVIIICORPS.DS.ARMY.MIL	XVIIICORPS.DS.ARMY.SMIL.MIL	XVIIICORPS
Divisions			
1AD	1AD.DS.ARMY.MIL	1AD.DS.ARMY.SMIL.MIL	1AD
1BCT1AD	1BCT1AD.DS.ARMY.MIL	1BCT1AD.DS.ARMY.SMIL.MIL	1BCT1AD

2BCT1AD	2BCT1AD.DS.ARMY.MIL	2BCT1AD.DS.ARMY.SMIL.MIL	2BCT1AD

Table A-2. Forest names, domain names, and exchange organization names of active component tactical deployable units (continued)

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
Divisions			
3BCT1AD	3BCT1AD.DS.ARMY.MIL	3BCT1AD.DS.ARMY.SMIL.MIL	3BCT1AD
4BCT1AD	4BCT1AD.DS.ARMY.MIL	4BCT1AD.DS.ARMY.SMIL.MIL	4BCT1AD
1CAB1AD	1CAB1AD.DS.ARMY.MIL	1CAB1AD.DS.ARMY.SMIL.MIL	1CAB1AD
1CD	1CD.DS.ARMY.MIL	1CD.DS.ARMY.SMIL.MIL	1CD
1BCT1CD	1BCT1CD.DS.ARMY.MIL	1BCT1CD.DS.ARMY.SMIL.MIL	1BCT1CD
2BCT1CD	2BCT1CD.DS.ARMY.MIL	2BCT1CD.DS.ARMY.SMIL.MIL	2BCT1CD
3BCT1CD	3BCT1CD.DS.ARMY.MIL	3BCT1CD.DS.ARMY.SMIL.MIL	3BCT1CD
4BCT1CD	4BCT1CD.DS.ARMY.MIL	4BCT1CD.DS.ARMY.SMIL.MIL	4BCT1CD
1CAB1CD	1CAB1CD.DS.ARMY.MIL	1CAB1CD.DS.ARMY.SMIL.MIL	1CAB1CD
1ID	1ID.DS.ARMY.MIL	1ID.DS.ARMY.SMIL.MIL	1ID
1BCT1ID	1BCT1ID.DS.ARMY.MIL	1BCT1ID.DS.ARMY.SMIL.MIL	1BCT1ID
2BCT1ID	2BCT1ID.DS.ARMY.MIL	2BCT1ID.DS.ARMY.SMIL.MIL	2BCT1ID
3BCT1ID	3BCT1ID.DS.ARMY.MIL	3BCT1ID.DS.ARMY.SMIL.MIL	3BCT1ID
4BCT1ID	4BCT1ID.DS.ARMY.MIL	4BCT1ID.DS.ARMY.SMIL.MIL	4BCT1ID
1CAB1ID	1CAB1ID.DS.ARMY.MIL	1CAB1ID.DS.ARMY.SMIL.MIL	1CAB1ID
2ID	2ID.DS.ARMY.MIL	2ID.DS.ARMY.SMIL.MIL	2ID
1BCT2ID	1BCT2ID.DS.ARMY.MIL	1BCT2ID.DS.ARMY.SMIL.MIL	1BCT2ID
2BCT2ID	2BCT2ID.DS.ARMY.MIL	2BCT2ID.DS.ARMY.SMIL.MIL	2BCT2ID
3BCT2ID	3BCT2ID.DS.ARMY.MIL	3BCT2ID.DS.ARMY.SMIL.MIL	3BCT2ID
4BCT2ID	4BCT2ID.DS.ARMY.MIL	4BCT2ID.DS.ARMY.SMIL.MIL	4BCT2ID
2CAB2ID	2CAB2ID.DS.ARMY.MIL	2CAB2ID.DS.ARMY.SMIL.MIL	2CAB2ID
3ID	3ID.DS.ARMY.MIL	3ID.DS.ARMY.SMIL.MIL	3ID
1BCT3ID	1BCT3ID.DS.ARMY.MIL	1BCT3ID.DS.ARMY.SMIL.MIL	1BCT3ID
2BCT3ID	2BCT3ID.DS.ARMY.MIL	2BCT3ID.DS.ARMY.SMIL.MIL	2BCT3ID
3BCT3ID	3BCT3ID.DS.ARMY.MIL	3BCT3ID.DS.ARMY.SMIL.MIL	3BCT3ID
4BCT3ID	4BCT3ID.DS.ARMY.MIL	4BCT3ID.DS.ARMY.SMIL.MIL	4BCT3ID
3CAB3ID	3CAB3ID.DS.ARMY.MIL	3CAB3ID.DS.ARMY.SMIL.MIL	3CAB3ID
4ID	4ID.DS.ARMY.MIL	4ID.DS.ARMY.SMIL.MIL	4ID
1BCT4ID	1BCT4ID.DS.ARMY.MIL	1BCT4ID.DS.ARMY.SMIL.MIL	1BCT4ID
2BCT4ID	2BCT4ID.DS.ARMY.MIL	2BCT4ID.DS.ARMY.SMIL.MIL	2BCT4ID
3BCT4ID	3BCT4ID.DS.ARMY.MIL	3BCT4ID.DS.ARMY.SMIL.MIL	3BCT4ID
4BCT4ID	4BCT4ID.DS.ARMY.MIL	4BCT4ID.DS.ARMY.SMIL.MIL	4BCT4ID
4CAB4ID	4CAB4ID.DS.ARMY.MIL	4CAB4ID.DS.ARMY.SMIL.MIL	4CAB4ID
7ID	7ID.DS.ARMY.MIL	7ID.DS.ARMY.SMIL.MIL	7ID
10ID	10ID.DS.ARMY.MIL	10ID.DS.ARMY.SMIL.MIL	10ID
1BCT10ID	1BCT10ID.DS.ARMY.MIL	1BCT10ID.DS.ARMY.SMIL.MIL	1BCT10ID
2BCT10ID	2BCT10ID.DS.ARMY.MIL	2BCT10ID.DS.ARMY.SMIL.MIL	2BCT10ID
3BCT10ID	3BCT10ID.DS.ARMY.MIL	3BCT10ID.DS.ARMY.SMIL.MIL	3BCT10ID

4BCT10ID	4BCT10ID.DS.ARMY.MIL	4BCT10ID.DS.ARMY.SMIL.MIL	4BCT10ID

Table A-2. Forest names, domain names, and exchange organization names of active component tactical deployable units (continued)

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
Divisions			
10CAB10ID	10CAB10ID.DS.ARMY.MIL	10CAB10ID.DS.ARMY.SMIL.MIL	10CAB10ID
24ID	24ID.DS.ARMY.MIL	24ID.DS.ARMY.SMIL.MIL	24ID
25ID	25ID.DS.ARMY.MIL	25ID.DS.ARMY.SMIL.MIL	25ID
1BCT25ID	1BCT25ID.DS.ARMY.MIL	1BCT25ID.DS.ARMY.SMIL.MIL	1BCT25ID
2BCT25ID	2BCT25ID.DS.ARMY.MIL	2BCT25ID.DS.ARMY.SMIL.MIL	2BCT25ID
3BCT25ID	3BCT25ID.DS.ARMY.MIL	3BCT25ID.DS.ARMY.SMIL.MIL	3BCT25ID
4BCT25ID	4BCT25ID.DS.ARMY.MIL	4BCT25ID.DS.ARMY.SMIL.MIL	4BCT25ID
25CAB25ID	25CAB25ID.DS.ARMY.MIL	25CAB25ID.DS.ARMY.SMIL.MIL	25CAB25ID
82AB	82AB.DS.ARMY.MIL	82AB.DS.ARMY.SMIL.MIL	82AB
1BCT82AB	1BCT82AB.DS.ARMY.MIL	1BCT82AB.DS.ARMY.SMIL.MIL	1BCT82AB
2BCT82AB	2BCT82AB.DS.ARMY.MIL	2BCT82AB.DS.ARMY.SMIL.MIL	2BCT82AB
3BCT82AB	3BCT82AB.DS.ARMY.MIL	3BCT82AB.DS.ARMY.SMIL.MIL	3BCT82AB
4BCT82AB	4BCT82AB.DS.ARMY.MIL	4BCT82AB.DS.ARMY.SMIL.MIL	4BCT82AB
82CAB82AB	82CAB82AB.DS.ARMY.MIL	82CAB82AB.DS.ARMY.SMIL.MIL	82CAB82AB
101AA	101AA.DS.ARMY.MIL	101AA.DS.ARMY.SMIL.MIL	101AA
1BCT101AA	1BCT101AA.DS.ARMY.MIL	1BCT101AA.DS.ARMY.SMIL.MIL	1BCT101AA
2BCT101AA	2BCT101AA.DS.ARMY.MIL	2BCT101AA.DS.ARMY.SMIL.MIL	2BCT101AA
3BCT101AA	3BCT101AA.DS.ARMY.MIL	3BCT101AA.DS.ARMY.SMIL.MIL	3BCT101AA
4BCT101AA	4BCT101AA.DS.ARMY.MIL	4BCT101AA.DS.ARMY.SMIL.MIL	4BCT101AA
101CAB101AA	101CAB101AA.DS.ARMY.MIL	101CAB101AA.DS.ARMY.SMIL.MIL	101CAB101AA
159CAB101AA	159CAB101AA.DS.ARMY.MIL	159CAB101AA.DS.ARMY.SMIL.MIL	159CAB101AA
Separate Brigades			
173ABBCT	173ABBCT.DS.ARMY.MIL	173ABBCT.DS.ARMY.SMIL.MIL	173ABBCT
2ACRCT	2ACRCT.DS.ARMY.MIL	2ACRCT.DS.ARMY.SMIL.MIL	2ACRCT
3ACRCT	3ACRCT.DS.ARMY.MIL	3ACRCT.DS.ARMY.SMIL.MIL	3ACRCT
11ACRCT	11ACRCT.DS.ARMY.MIL	11ACRCT.DS.ARMY.SMIL.MIL	11ACRCT
12CAB	12CAB.DS.ARMY.MIL	12CAB.DS.ARMY.SMIL.MIL	12CAB
Fires Brigades			
4FSBDE	4FSBDE.DS.ARMY.MIL	4FSBDE.DS.ARMY.SMIL.MIL	4FSBDE
17FSBDE	17FSBDE.DS.ARMY.MIL	17FSBDE.DS.ARMY.SMIL.MIL	17FSBDE
18FSBDE	18FSBDE.DS.ARMY.MIL	18FSBDE.DS.ARMY.SMIL.MIL	18FSBDE
75FSBDE	75FSBDE.DS.ARMY.MIL	75FSBDE.DS.ARMY.SMIL.MIL	75FSBDE
212FSBDE	212FSBDE.DS.ARMY.MIL	212FSBDE.DS.ARMY.SMIL.MIL	212FSBDE
214FSBDE	214FSBDE.DS.ARMY.MIL	214FSBDE.DS.ARMY.SMIL.MIL	214FSBDE
CS Brigades (ME) (On 07 Nov 07, HQDA approved the re-designation of the Combat Support Brigade (Maneuver Enhancement) to the "Maneuver Enhancement Brigade (MEB)).			
1CSBDEME	1CSBDEME.DS.ARMY.MIL	1CSBDEME.DS.ARMY.SMIL.MIL	1CSBDEME
2CSBDEME	2CSBDEME.DS.ARMY.MIL	2CSBDEME.DS.ARMY.SMIL.MIL	2CSBDEME

3CSBDEME	3CSBDEME.DS.ARMY.MIL	3CSBDEME.DS.ARMY.SMIL.MIL	3CSBDEME

Table A-2. Forest names, domain names, and exchange organization names of active component tactical deployable units (continued)

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
Sustainment Brigades			
1CSBDE	1CSBDE.DS.ARMY.MIL	1CSBDE.DS.ARMY.SMIL.MIL	1CSBDE
3CSBDE	3CSBDE.DS.ARMY.MIL	3CSBDE.DS.ARMY.SMIL.MIL	3CSBDE
4CSBDE	4CSBDE.DS.ARMY.MIL	4CSBDE.DS.ARMY.SMIL.MIL	4CSBDE
7CSBDE	7CSBDE.DS.ARMY.MIL	7CSBDE.DS.ARMY.SMIL.MIL	7CSBDE
10CSBDE	10CSBDE.DS.ARMY.MIL	10CSBDE.DS.ARMY.SMIL.MIL	10CSBDE
15CSBDE	15CSBDE.DS.ARMY.MIL	15CSBDE.DS.ARMY.SMIL.MIL	15CSBDE
16CSBDE	16CSBDE.DS.ARMY.MIL	16CSBDE.DS.ARMY.SMIL.MIL	16CSBDE
29CSBDE	29CSBDE.DS.ARMY.MIL	29CSBDE.DS.ARMY.SMIL.MIL	29CSBDE
43CSBDE	43CSBDE.DS.ARMY.MIL	43CSBDE.DS.ARMY.SMIL.MIL	43CSBDE
45CSBDE	45CSBDE.DS.ARMY.MIL	45CSBDE.DS.ARMY.SMIL.MIL	45CSBDE
64CSBDE	64CSBDE.DS.ARMY.MIL	64CSBDE.DS.ARMY.SMIL.MIL	64CSBDE
82CSBDE	82CSBDE.DS.ARMY.MIL	82CSBDE.DS.ARMY.SMIL.MIL	82CSBDE
101CSBDE	101CSBDE.DS.ARMY.MIL	101CSBDE.DS.ARMY.SMIL.MIL	101CSBDE
501CSBDE	501CSBDE.DS.ARMY.MIL	501CSBDE.DS.ARMY.SMIL.MIL	501CSBDE
507CSBDE	507CSBDE.DS.ARMY.MIL	507CSBDE.DS.ARMY.SMIL.MIL	507CSBDE
593CSBDE	593CSBDE.DS.ARMY.MIL	593CSBDE.DS.ARMY.SMIL.MIL	593CSBDE

Table A-3. Forest names, domain names, and exchange organization names of National Guard tactical deployable units

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
Divisions			
28ID	28ID.DS.ARMY.MIL	28ID.DS.ARMY.SMIL.MIL	28ID
2BCT28ID	2BCT28ID.DS.ARMY.MIL	2BCT28ID.DS.ARMY.SMIL.MIL	2BCT28ID
55BCT28ID	55BCT28ID.DS.ARMY.MIL	55BCT28ID.DS.ARMY.SMIL.MIL	55BCT28ID
56BCT28ID	56BCT28ID.DS.ARMY.MIL	56BCT28ID.DS.ARMY.SMIL.MIL	56BCT28ID
28CAB28ID	28CAB28ID.DS.ARMY.MIL	28CAB28ID.DS.ARMY.SMIL.MIL	28CAB28ID
29ID	29ID.DS.ARMY.MIL	29ID.DS.ARMY.SMIL.MIL	29ID
116BCT29ID	116BCT29ID.DS.ARMY.MIL	116BCT29ID.DS.ARMY.SMIL.MIL	116BCT29ID
29CAB29ID	29CAB29ID.DS.ARMY.MIL	29CAB29ID.DS.ARMY.SMIL.MIL	29CAB29ID
34ID	34ID.DS.ARMY.MIL	34ID.DS.ARMY.SMIL.MIL	34ID
1BCT34ID	1BCT34ID.DS.ARMY.MIL	1BCT34ID.DS.ARMY.SMIL.MIL	1BCT34ID
2BCT34ID	2BCT34ID.DS.ARMY.MIL	2BCT34ID.DS.ARMY.SMIL.MIL	2BCT34ID
34CAB34ID	34CAB34ID.DS.ARMY.MIL	34CAB34ID.DS.ARMY.SMIL.MIL	34CAB34ID
35ID	35ID.DS.ARMY.MIL	35ID.DS.ARMY.SMIL.MIL	35ID
35CAB35ID	35CAB35ID.DS.ARMY.MIL	35CAB35ID.DS.ARMY.SMIL.MIL	35CAB35ID
36ID	36ID.DS.ARMY.MIL	36ID.DS.ARMY.SMIL.MIL	36ID

56BCT36ID	56BCT36ID.DS.ARMY.MIL	56BCT36ID.DS.ARMY.SMIL.MIL	56BCT36ID

Table A-3. Forest names, domain names, and exchange organization names of National Guard tactical deployable units (continued)

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
72BCT36ID	72BCT36ID.DS.ARMY.MIL	72BCT36ID.DS.ARMY.SMIL.MIL	72BCT36ID
36CAB36ID	36CAB36ID.DS.ARMY.MIL	36CAB36ID.DS.ARMY.SMIL.MIL	36CAB36ID
38ID	38ID.DS.ARMY.MIL	38ID.DS.ARMY.SMIL.MIL	38ID
38CAB38ID	38CAB38ID.DS.ARMY.MIL	38CAB38ID.DS.ARMY.SMIL.MIL	38CAB38ID
40ID	40ID.DS.ARMY.MIL	40ID.DS.ARMY.SMIL.MIL	40ID
2BCT40ID	2BCT40ID.DS.ARMY.MIL	2BCT40ID.DS.ARMY.SMIL.MIL	2BCT40ID
40CAB40ID	40CAB40ID.DS.ARMY.MIL	40CAB40ID.DS.ARMY.SMIL.MIL	40CAB40ID
42ID	42ID.DS.ARMY.MIL	42ID.DS.ARMY.SMIL.MIL	42ID
27BCT42ID	27BCT42ID.DS.ARMY.MIL	27BCT42ID.DS.ARMY.SMIL.MIL	27BCT42ID
42CAB42ID	42CAB42ID.DS.ARMY.MIL	42CAB42ID.DS.ARMY.SMIL.MIL	42CAB42ID
Separate Brigades			
116ACRCT	116ACRCT.DS.ARMY.MIL	116ACRCT.DS.ARMY.SMIL.MIL	116ACRCT
149BCT	149BCT.DS.ARMY.MIL	149BCT.DS.ARMY.SMIL.MIL	149BCT
155BCT	155BCT.DS.ARMY.MIL	155BCT.DS.ARMY.SMIL.MIL	155BCT
207BCT	207BCT.DS.ARMY.MIL	207BCT.DS.ARMY.SMIL.MIL	207BCT
218BCT	218BCT.DS.ARMY.MIL	218BCT.DS.ARMY.SMIL.MIL	218BCT
256BCT	256BCT.DS.ARMY.MIL	256BCT.DS.ARMY.SMIL.MIL	256BCT
26BCT	26BCT.DS.ARMY.MIL	26BCT.DS.ARMY.SMIL.MIL	26BCT
278ACRCT	278ACRCT.DS.ARMY.MIL	278ACRCT.DS.ARMY.SMIL.MIL	278ACRCT
29BCT	29BCT.DS.ARMY.MIL	29BCT.DS.ARMY.SMIL.MIL	29BCT
30BCT	30BCT.DS.ARMY.MIL	30BCT.DS.ARMY.SMIL.MIL	30BCT
32BCT	32BCT.DS.ARMY.MIL	32BCT.DS.ARMY.SMIL.MIL	32BCT
33BCT	33BCT.DS.ARMY.MIL	33BCT.DS.ARMY.SMIL.MIL	33BCT
37BCT	37BCT.DS.ARMY.MIL	37BCT.DS.ARMY.SMIL.MIL	37BCT
39BCT	39BCT.DS.ARMY.MIL	39BCT.DS.ARMY.SMIL.MIL	39BCT
41BCT	41BCT.DS.ARMY.MIL	41BCT.DS.ARMY.SMIL.MIL	41BCT
45BCT	45BCT.DS.ARMY.MIL	45BCT.DS.ARMY.SMIL.MIL	45BCT
48BCT	48BCT.DS.ARMY.MIL	48BCT.DS.ARMY.SMIL.MIL	48BCT
50BCT	50BCT.DS.ARMY.MIL	50BCT.DS.ARMY.SMIL.MIL	50BCT
53BCT	53BCT.DS.ARMY.MIL	53BCT.DS.ARMY.SMIL.MIL	53BCT
58BCT	58BCT.DS.ARMY.MIL	58BCT.DS.ARMY.SMIL.MIL	58BCT
76BCT	76BCT.DS.ARMY.MIL	76BCT.DS.ARMY.SMIL.MIL	76BCT
81BCT	81BCT.DS.ARMY.MIL	81BCT.DS.ARMY.SMIL.MIL	81BCT
86BCT	86BCT.DS.ARMY.MIL	86BCT.DS.ARMY.SMIL.MIL	86BCT
92BCT	92BCT.DS.ARMY.MIL	92BCT.DS.ARMY.SMIL.MIL	92BCT

Table A-3. Forest names, domain names, and exchange organization names of National Guard tactical deployable units (continued)

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
Fires Brigades			
45FSBDE	45FSBDE.DS.ARMY.MIL	45FSBDE.DS.ARMY.SMIL.MIL	45FSBDE
65FSBDE	65FSBDE.DS.ARMY.MIL	65FSBDE.DS.ARMY.SMIL.MIL	65FSBDE
138FSBDE	138FSBDE.DS.ARMY.MIL	138FSBDE.DS.ARMY.SMIL.MIL	138FSBDE
142FSBDE	142FSBDE.DS.ARMY.MIL	142FSBDE.DS.ARMY.SMIL.MIL	142FSBDE
169FSBDE	169FSBDE.DS.ARMY.MIL	169FSBDE.DS.ARMY.SMIL.MIL	169FSBDE
197FSBDE	197FSBDE.DS.ARMY.MIL	197FSBDE.DS.ARMY.SMIL.MIL	197FSBDE
CS Brigades (ME)			
110CSBDEME	110CSBDEME.DS.ARMY.MIL	110CSBDEME.DS.ARMY.SMIL.MIL	110CSBDEME
111CSBDEME	111CSBDEME.DS.ARMY.MIL	111CSBDEME.DS.ARMY.SMIL.MIL	111CSBDEME
130CSBDEME	130CSBDEME.DS.ARMY.MIL	130CSBDEME.DS.ARMY.SMIL.MIL	130CSBDEME
136CSBDEME	136CSBDEME.DS.ARMY.MIL	136CSBDEME.DS.ARMY.SMIL.MIL	136CSBDEME
142CSBDEME	142CSBDEME.DS.ARMY.MIL	142CSBDEME.DS.ARMY.SMIL.MIL	142CSBDEME
157CSBDEME	157CSBDEME.DS.ARMY.MIL	157CSBDEME.DS.ARMY.SMIL.MIL	157CSBDEME
225CSBDEME	225CSBDEME.DS.ARMY.MIL	225CSBDEME.DS.ARMY.SMIL.MIL	225CSBDEME
Sustainment Brigades			
34CSBDE	34CSBDE.DS.ARMY.MIL	34CSBDE.DS.ARMY.SMIL.MIL	34CSBDE
36CSBDE	36CSBDE.DS.ARMY.MIL	36CSBDE.DS.ARMY.SMIL.MIL	36CSBDE
38CSBDE	38CSBDE.DS.ARMY.MIL	38CSBDE.DS.ARMY.SMIL.MIL	38CSBDE
40CSBDE	40CSBDE.DS.ARMY.MIL	40CSBDE.DS.ARMY.SMIL.MIL	40CSBDE
67CSBDE	67CSBDE.DS.ARMY.MIL	67CSBDE.DS.ARMY.SMIL.MIL	67CSBDE
108CSBDE	108CSBDE.DS.ARMY.MIL	108CSBDE.DS.ARMY.SMIL.MIL	108CSBDE
230CSBDE	230CSBDE.DS.ARMY.MIL	230CSBDE.DS.ARMY.SMIL.MIL	230CSBDE
287CSBDE	287CSBDE.DS.ARMY.MIL	287CSBDE.DS.ARMY.SMIL.MIL	287CSBDE
369CSBDE	369CSBDE.DS.ARMY.MIL	369CSBDE.DS.ARMY.SMIL.MIL	369CSBDE
371CSBDE	371CSBDE.DS.ARMY.MIL	371CSBDE.DS.ARMY.SMIL.MIL	371CSBDE

Table A-4 Forest names, domain names, and exchange organization names of US Army Reserve tactical deployable units

Forest Name	*NIPR Domain name (one per forest only)*	*SIPR Domain name (one per forest only)*	*Exchange Organization name SIPR and NIPR*
CS Brigades (ME)			
301CSBDEME	301CSBDEME.DS.ARMY.MIL	301CSBDEME.DS.ARMY.SMIL.MIL	301CSBDEME
302CSBDEME	302CSBDEME.DS.ARMY.MIL	302CSBDEME.DS.ARMY.SMIL.MIL	302CSBDEME
303CSBDEME	303CSBDEME.DS.ARMY.MIL	303CSBDEME.DS.ARMY.SMIL.MIL	303CSBDEME
Sustainment Brigades			
55CSBDE	55CSBDE.DS.ARMY.MIL	55CSBDE.DS.ARMY.SMIL.MIL	55CSBDE
158CSBDE	158CSBDE.DS.ARMY.MIL	158CSBDE.DS.ARMY.SMIL.MIL	158CSBDE

Table A-4 Forest names, domain names, and exchange organization names of US Army Reserve tactical deployable units (continued)			
Forest Name	***NIPR Domain name (one per forest only)***	***SIPR Domain name (one per forest only)***	***Exchange Organization name SIPR and NIPR***
162CSBDE	162CSBDE.DS.ARMY.MIL	162CSBDE.DS.ARMY.SMIL.MIL	162CSBDE
164CSBDE	164CSBDE.DS.ARMY.MIL	164CSBDE.DS.ARMY.SMIL.MIL	164CSBDE
300CSBDE	300CSBDE.DS.ARMY.MIL	300CSBDE.DS.ARMY.SMIL.MIL	300CSBDE
304CSBDE	304CSBDE.DS.ARMY.MIL	304CSBDE.DS.ARMY.SMIL.MIL	304CSBDE
321CSBDE	321CSBDE.DS.ARMY.MIL	321CSBDE.DS.ARMY.SMIL.MIL	321CSBDE
474CSBDE	474CSBDE.DS.ARMY.MIL	474CSBDE.DS.ARMY.SMIL.MIL	474CSBDE

A-40. Tables A-5 through A-7 are the abbreviations used in Tables A-2 through A-4, respectively.

Table A-5. Abbreviations for Table A-2

Active Component	***Abbreviation***
1st Armored Division	1AD
1st Cavalry Division	1CD
1st Infantry Division	1ID
2d Infantry Division	2ID
3d Infantry Division	3ID
4th Infantry Division	4ID
7th Infantry Division	7ID
10th Infantry Division	10ID
24th Infantry Division	24ID
25th Infantry Division	25ID
82d Airborne Division	82AB
101st Air Assault Division	101AA

Table A-6. Abbreviations for Table A-3

Army National Guard/Reserve	***Abbreviation***
28th Infantry Division	28ID
29th Infantry Division	29ID
34th Infantry Division	34ID
35th Infantry Division	35ID
36th Infantry Division (old 49AD)	36ID
38th Infantry Division	38ID
40th Infantry Division	40ID
42d Infantry Division	42ID

Table A-7. Abbreviations for Table A-4

Term	*Abbreviation*
Air Assault	AA
Airborne	AB
Airborne Brigade Combat Team	ABCT
Armored Cavalry Regiment Combat Team	ACRCT
Air Defense	AD
Brigade Combat Team	BCT
Brigade	BDE
Combat Aviation Brigade	CAB
Cavalry Division	CD
Combat Support	CS
Fire Support	FS
Infantry Division	ID
Maneuver Enhancement	ME
Multi-Function Aviation Brigade	MFAB

Appendix B

NETWORK OPERATIONS SYSTEMS AND TOOLS

This appendix addresses the different systems and tools available to perform the required NETOPS functions. It is separated by the tools used in the A-GNOSC and TNOSC and into three other distinct areas: ESM/NM, IA/CND, and IDM/CS.

APPROVED NETWORK OPERATIONS TOOLS FOR NETWORK OPERATIONS AND SECURITY CENTERS.

B-1. The list in Table B-1 defines the minimum approved NETOPS tools for use in the AGNOSCs and TNOSCs with respect to capabilities outlined in the AENIA. This list will be reviewed on a quarterly basis or sooner, if required.

B-2. The NETCOM Chief, NETOPS Planning Division will establish an action officer level NOSC working group under the AEI Technical Configuration Control Board. The NOSC working group will include representation from the requirements, material development and user communities. The NOSC working group will establish specific CIs; manage specific changes and updates to the listed set of tools via a CM process.

B-3. NOSCs not operating on these standard tools will develop migration plans ICW the NOSC working group to comply with the stated standard.

B-4. Functional Proponent for the AENIA and NOSC NETOPS tools is the chief, NETOPS planning division NETCOM at commercial: (520) 533-1 852, DSN: 821-1852.

Table B-1. A-GNOSC and TNOSC NETOPS tools list

AENIA Capability	*Capability Description*	*NOSC Standard*	*Comments*
Anti-Virus (Anti-Malware)	This system provides an enterprise view and management capability for anti-virus and anti-malware.	Three DOD Anti-Virus standards: Symantec, McAfee, and TrendMicro. DOD CND enterprise-wide solutions steering group has selected McAfee ePolicy Orchestrator Entercept as standard for Host-Based Security System which includes anti-virus management and Computer Associates Pest Patrol to provide a standard Adware/Spyware capability.	McAfee ePolicy Orchestrator Entercept is undergoing DISA/Army pilot.

Table B-1. A-GNOSC and TNOSC NETOPS tools list (continued)

AENIA Capability	*Capability Description*	*NOSC Standard*	*Comments*
Capacity, Availability and Performance Monitoring System	This system provides the capability to monitor and analyze capacity and availability information collected by other systems and stored in this system.	eHealth (Computer Associates)	Additional capacity, availability and performance monitoring tool standards are anticipated to support this capability.
CM Database/Support System	This system provides a great deal of functionality. The functionality can be broken down into 4 broad areas: incident/problem/service request management, operational asset management, change management and other supporting features.	Remedy Information Technology Service Management	
Host IDS	This system provides the capability for an agent to monitor host activities and identify those activities that have been identified as being potentially hostile. The potentially hostile activities are reported to a management console for analysis.	Symantec Intruder Alert/Enterprise Security Manager DOD CND enterprise-wide solutions steering group has selected McAfee ePolicy Orchestrator/Entercept as standard under the Host-Based Security System initiative to provide a standard host intrusion detection and host-based firewall capability.	The current standard for Host IDS/ Host Intrusion Prevention System is Symantec Intruder Alert/Enterprise Security Manager. NETCOM will migrate to the DISA/Army Host-Based Security System standard upon successful completion of the DISN/Army pilot.

Table B-1. A-GNOSC and TNOSC NETOPS tools list (continued)

AENIA Capability	*Capability Description*	*NOSC Standard*	*Comments*
Host Intrusion Prevention System	This system provides the capability for an agent to monitor host activities and identify potentially hostile activities. Predefined remedial actions are then taken to mitigate the impact of these activities on the operational system. The identification and mitigation of potentially hostile activities are reported to a management console for analysis.	Symantec Intruder Alert/Enterprise Security Manager DOD CND enterprise-wide solutions steering group has selected McAfee ePolicy Orchestrator/Entercept as standard under the Host-Based Security System initiative to provide a standard host intrusion prevention and host-based firewall capability.	The current standard for Host IDS/Host Intrusion Prevention System is Symantec Intruder Alert/Enterprise Security Manager. NETCOM will migrate to the DISA/Army Host-Based Security System standard upon successful completion of the DISA/Army pilot.
IP Network Management System	This system provides a network monitoring and graphical display capability. It is the only system that collects Simple Network Management Protocol data from devices connected to the network.	Spectrum Network Management System (Computer Associates)	
SA	This system provides the capability for non-IT staff to understand the impact of IT services on the theater's operational mission. It receives status information from sources external to the Army from the Army level situation awareness System. The situation awareness at the Army level receives status information from sources external to the Army and passes this external status information to the theater situation awareness.	Formula (Managed Objects)	

Table B-1. A-GNOSC and TNOSC NETOPS tools list (continued)

AENIA Capability	*Capability Description*	*NOSC Standard*	*Comments*
Network IDS	This system provides the capability for an agent or device to monitor network traffic and to identify traffic that has been identified as being potentially hostile. The potentially hostile traffic is reported to a management console for analysis.	Internet Security Systems SiteProtector; Snort	NETCOM has initiated a plan to replace existing Network IDS with Network Intrusion Prevention Systems.
Network Intrusion Prevention System	This system provides the capability for an agent or device to monitor network traffic and to identify and mitigate traffic that has been identified as being potentially hostile. The potentially hostile traffic is reported to a management console for analysis	To Be Determined	NETCOM has initiated a plan to replace existing Network IDSs with Network Intrusion Prevention Systems.
Secure Configuration Remediation (Patch) Management	This system provides the capability to define configuration conditions and responses. It may change system configuration or install patches to existing software.	Citadel Hercules Windows Environment-Microsoft Systems Management Server	Citadel Hercules selected by DOD CND enterprise-wide solutions steering group. DOD acquisition includes Enterprise License for software, and on-line training. Systems Management Server 3rd Party Bolt-on being considered for Non-Windows Environment Enterprise solution.

Table B-1. A-GNOSC and TNOSC NETOPS tools list (continued)

AENIA Capability	*Capability Description*	*NOSC Standard*	*Comments*
Security Information Management System	This system provides the capability to receive events from a large number of other commercial operations and security related products. These events are then correlated to all of the other events it has received from all of its other sources.	Arcsight (Arcsight)	DOD CND enterprise-wide solutions steering group is currently researching a Tier 3 Systems Management Server solution to support post/camp/station and enclaves.
Systems Management	This system provides the capability to monitor and manage various aspects of computing platforms (both servers and desktops). It provides an inventory and configuration capability, a software distribution capability, and a condition monitoring capability.	Windows Desktop Environment-Microsoft Systems Management Server Windows Server Environment-Microsoft Systems Management Server and Microsoft Operations Management	Systems Management Server/Microsoft Operations Management 3rd Party Bolt-on being considered for Non-Windows Environment Enterprise solution.
IP Network Vulnerability Scanner	This system provides the capability to define a number of different scanning profiles. These scanning profiles should be related to the compliance baselines established in the compliance manager. The system then interrogates systems using a number of different means to determine how vulnerable the system is to the scanning criteria.	eEye Retina	eEye Retina selected by DOD CND enterprise-wide solutions steering group. DOD acquisition includes Enterprise License for software, and on-line training.

GLOBAL INFORMATION GRID ENTERPRISE MANAGEMENT AND LANDWARNET SYSTEMS AND TOOLS

B-5. The ESM/NM and LWN systems and tools will be available to the management personnel. Many of the systems and tools may be listed more than once due to the tool being a subsystem to other management systems as well as a stand alone tool used for other functions in the networks. The NM/ESM and LWN systems and tools are:

- CISCO Call Manager is a software-based call processing component providing signaling and call control services to Cisco integrated telephony applications (e.g., VG-248 subscribers, Cisco IP Phones, or Cisco IP softphones). The Call Manager also registers with the Vantage as a gateway.

The JNN Call Manager is physically associated to a particular security domain by keyboard video monitor and Ethernet connectivity to that domain. The JNN Call Manager software function is hosted on a rack mounted computer and has a single Ethernet connection to the Tier 2 router Ethernet switch module. There are two Call Managers in the shelter: one dedicated for NIPR and another for SIPR.

- Cisco Call Manager Version 3.3(2) software provides the call management function. The Cisco Call Manager's primary functions are: call processing, signaling and device control, dial plan administration, and phone feature administration. The Cisco Call Manager is a main component in the shelter voice architecture.

B-6. Network Management-Element and Node Planning and Management platform is present within each security domain (NIPR and SIPR). The node manager provides monitoring and control capabilities reporting on the condition of the router and network components. In addition, the node manager platform provides the capability to build and save Cisco device configurations (router's and firewall) based upon mission specific criteria. A Denika Multi-Router Traffic Grapher application shall be provided for the purpose of monitoring bandwidth utilization. The JNN manager platform is designed to operate on a laptop computer with the following software installed:

- Ciscoworks for Small Network Management Systems includes:
  - Resource Manager Essentials 3.3.
  - CiscoView 5.3.
- WhatsUp Gold.
- Multi-Router Traffic Grapher v3.0.1.210.
- Warfighter Machine Interface.

B-7. CiscoWorks for Small Network Management Systems is an end-to-end network management solution. It is ideal for small networks that may include two or three branches. It also provides management capabilities that simplify network administration. CiscoWorks for Small Network Management Systems enables network operators to efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime and anywhere within the network. CiscoWorks for Small Network Management Systems provides tools that make the job of configuring, monitoring, and troubleshooting routers and switches quicker in order to reduce the likelihood of human errors.

B-8. The functionality of CiscoWorks for Small Network Management Systems can be categorized under three functional areas: network discovery and policy management, device configuration, and device management. Network discovery and policy management is performed using the WhatsUp Gold software package. Device configuration tasks are performed using the CiscoView software package, and device management is performed using the Resource Manager Essentials software package.

B-9. Resource Manager Essentials 3.3 is a suite of Web-based applications offering network management solutions for Cisco switches, access servers, and routers. Resource Manager Essentials is comprised of several applications which are discussed below.

B-10. The inventory manager, is responsible for—

- Up-to-date inventory of all Cisco devices in the network.
- Hardware and software summary information as well as detailed reports for groups of devices, including device name, chassis type, memory, flash, and software version or characteristics.
- Capacity planning information by identifying the total number of free and used slots in many Cisco devices.
- Multi-service port report on the number and location of Catalyst® switches that are multi-service port-enabled.

B-11. The device configuration manager maintains an active archive and simplifies deployment of configuration changes to multiple devices. It consists of the following subcomponents:

- Configuration Archive—

  - Maintains an up-to-date archive by automatically identifying and storing changes to configuration files.
  - Supports configuration file searching to simplify locating specific device configurations and configuration attributes.
  - Identifies differences between the running and startup configurations.
  - Has the ability to choose a device and its version of configuration and download it to the device from the configuration archive application.
- NetConfig—
  - Allows configuration changes to be performed against multiple switches or routers in the network; changes can be downloaded immediately or run as scheduled operations.
  - Provides flexibility in pushing command line interface changes out to the network via user-defined templates that are published to an authorized user or group of users for execution.
  - Has the ability for operators to specify username and password for devices selected for the job and during the job creation (functionality also available in ConfigEditor and NetShow).
- ConfigEditor provides a powerful Web-based editing facility for modifying and downloading configuration changes.
- NetShow provides a simplified Web-based show command interface, allowing show commands to be run against multiple switches or routers to enhance and simplify network troubleshooting.

B-12. The software image manager simplifies and speeds up software image analysis and deployment of software updates to the Cisco routers and switches through wizard-assisted planning, scheduling, downloading, and monitoring of software updates. The software image manager automates the many time-consuming steps required to upgrade software images while reducing the error-prone complexities of the upgrade process.

B-13. The change audit displays comprehensive reports of software, hardware, and configuration changes. Change audit is a central point where users can view network changes. Summary information is easily displayed, and shows the types of changes that are made. The information indicates who made the changes, when they were made, and if the changes were made from a telnet, console command-line interface, or a CiscoWorks application. Further, the nature of the changes is identified quickly through detailed reports (cards added or removed, memory changes, configuration changes, and so on).

B-14. The syslog analyzer isolates network error conditions and suggests probable causes. Syslog analyzer filters syslog messages logged by Cisco switches, routers, access servers, and Cisco Internet operating system firewalls, thus displaying explanations of probable causes and recommended actions. It leverages embedded Cisco Internet operating system technology to provide detailed device information.

B-15. The availability manager allows you to drill down on a particular device to view historical details about its response time, availability, reloads, protocols, and interface status.

B-16. CiscoView 5.3 is a Web-based device management application providing dynamic status, monitoring, and configuration information for Cisco internetworking products. CiscoView displays a physical view of a device chassis, with color-coding of modules and ports for visual status. Configuration capabilities allow comprehensive changes to devices given that requisite security privileges are granted.

B-17. WhatsUp Gold is a simple network management tool that enables the network manager to map and monitor the LAN and WAN. It also provides electronic notification and reporting of network changes, an interactive Web interface for remote viewing and administration, and a suite of network tools to help diagnose network problems.

B-18. The Denika Multi-Router Traffic Grapher v3.0.1.210 monitors the traffic load on network links and generates HTML pages containing graphical representations of live network traffic. Multi-Router Traffic

Grapher uses Simple Network Management Protocol to read router traffic counters log traffic data, and create traffic graphs for the monitored network connection.

B-19. The Enhanced Position Location Reporting System network manager (ENM) plans, configures, manages, and monitors the EPLRS network. It is the programmed replacement for the net control station—EPLRS, which is currently fielded to selected units in the Army. The ENM consists of two primary functions:

- **EPLRS network planner**: It is hosted on a laptop and is used to plan the EPLRS network, and provide key generation, platform configuration, and radio set configuration and reconfiguration. It is also used to initiate the timing master.
- **EPLRS network monitor**: It is hosted on a laptop located in G-6 or S-6 staff section. It provides configuration and cryptographic key files to forward deployed radios. It also provides monitoring and fault isolation of the ELPRS network.

B-20. The primary function of the ISYSCON (V) 4 is to configure and initialize network devices (locally or remotely) and disseminate configuration files to other ISYSCON (V) 4 in the network. The system will also monitor and perform fault management of the Army Battle Command System (ABCS) devices connected to the Tactical Internet, manage TOC and command post LANs, and monitor the status of the EPLRS and Blue Force Tracking (BFT) SA networks. It also performs critical changes to the network configuration and ensures distribution throughout the network. The ISYSCON (V) 4 package includes the Tactical Internet Management System, Force XXI Battle Command Brigade and Below (FBCB2) software 6.4.3, and Open Office 1.0.

B-21. The Tactical Information Management System is the backbone software package for the ISYSCON (V) 4. It provides the capability to plan, configure, and initialize network devices. It provides the graphical user interface that allows access to all other programs residing on the systems (ENM, WhatsUp Gold, etc.). It also provides the capability to perform unit task reorganization, which plans and implements changes to the initial network configuration for the Tactical Internet.

B-22. The FBCB2 6.4.3 software operates in the background of the ISYSCON (V) 4 enabling EPLRS and BFT the capability to provide SA and networks status monitoring. It allows the ISYSCON (V) 4 to function as the primary link between the FBCB2 centered Tactical Internet and other ABCS.

B-23. The Open Office 1.0 software enables the operator to create, edit, and print operational data reports. These reports detail the status and health of the LAN, FBCB2, or BFT SA networks. It includes tools typically found in office suite software bundles to include WRITER, CALC, IMPRESS, and DRAW. WRITER is a tool for creating documents, reports, newsletters, and brochures. You can integrate images and charts in documents, create letters, and create and publish Web content. CALC is a spreadsheet that can calculate and analyze data. IMPRESS is the multi-media presentation tool with special effects, animation, and high-impact drawing abilities. DRAW will produce everything from simple diagrams to dynamic 3D illustrations and special effects.

ISYSCON (V) 4 LITE

B-24. ISYSCON (V) 4 Lite provides the user with the capability to manually configure network devices and to monitor the local TOC LAN.

B-25. The Trivial File Transfer Protocol server allows configurations performed on the (V) 4 Lite to be transferred to the network devices through the LAN or a local connection.

B-26. WhatsUp Gold is a simple network management tool that enables the network manager to map and monitor the LAN and WAN. It also provides electronic notification and reporting of network changes, an interactive Web interface for remote viewing and administration, and a suite of network tools to help diagnose network problems.

ISYSCON (V) 1 AND 2

B-27. ISYSCON automates the coordination requirements for performing the essential functions of network management. It incorporates common hardware software workstations into a LAN that uses the Area Common User System to link all other ISYSCON shelters. It has Single-Channel Ground and Airborne Radio System (SINCGARS), EPLRS, and high frequency radio communications capabilities for use as the transmission means of linking ISYSCON elements. It supports planning, controlling, monitoring, and managing of tactical networks and communications assets, including tropospheric scatter radio, combat net radio, mobile subscriber equipment, tri-service tactical, SATCOM, high-speed data network, and commercial capabilities.

B-28. ISYSCON interfaces with other ISYSCONs operating on the same software version, with the Automated Communications Engineering Software, and will soon be interoperable with the Joint Network Management System. ISYSCON uses a standard database for frequency assignment function and Network Planning and Engineering. It performs WAN management and will allow a constant view of the network. ISYSCON stores and uses information regarding non-signal corps and non-communication emitters in managing the frequency assignment function. Its system management capabilities allow for the monitoring and managing of the communication network status and performance. ISYSCON provides a complete view of the battlefield WAN configuration and operational status in order to determine whether communication assets meet requirements and how best to employ for continuing operations. ISYSCON also supports the networks of other Armed Services and commercial systems.

Network Planning and Engineering

B-29. The network planning and engineering module uses new data to initiate development of new or modified mobile subscriber equipment network lay-downs to support the commander's directives. Once the lay-downs and plans are entered into the database, the frequency assignment function provides final engineering support of frequencies. The result of the network planning and engineering management, frequency assignment function, and COMSEC management processes becomes the basis for the communications plan. The network planning and engineering functions include data management (organization, task force, and equipment), link and site analysis, and asset planning. These functions facilitate the planning, design, and employment of communications networks. Considering terrain and tactical restrictions, this optimizes the placement of limited resources against subscriber requirements.

Detailed Planning and Engineering Module

B-30. The detailed planning and engineering module consists of hardware components and software applications. The hardware consists of a Tadpole V1 UNIX Laptop UltraSPARC IIi and the software consists primarily of the GNOME v2.0 application and the StarOffice v6.0 application suite.

Battlefield Spectrum Managment Module v 3.4

B-31. The battlefield spectrum management module manages frequency allotment, develops frequency assignments for tactical transmitters, and distributes those plans. It performs interference analysis and de-conflictions of those assigned frequencies.

Local Area Network and Wide Area Network Management Module

B-32. The LAN and WAN management module manages devices and events. It provides a graphical, near real-time representation of the WAN. The planned network selected for management is displayed with or without a map background. Event detection, translation, filtration, and dissemination activities control the presentation of the display. The network management center software has been ported on ISYSCON to perform comprehensive monitoring and centralized troubleshooting capabilities for the tactical packet network.

Mission Plan Management

B-33. The mission plan management module is where instructions and orders are developed. The module plans the required implementation of networks and systems, and prepares the command, control, communications, and computer operations annex to the OPORD or FRAGO, as required. The instructions (communications service orders) are transmitted to the responsible ISYSCONs for implementation. During pre-deployment, the communications service orders are printed and issued as team packets by the respective unit.

B-34. Each individual ISYSCON directs its networks to implement the communications service orders, and the communications network is established or modified. Upon network establishment, status reports are sent by users or automatically retrieved from communications terminals, switches, or other equipment back to the ISYSCON. These status reports that contain configuration, fault, and performance data are then provided to the WAN management function. The mission plan management module—

- Obtains the current network status.
- Synchronizes all network personnel assets to support operations.
- Develops deployment contingency plans.
- Generates and distributes deployment and redeployment plans and orders.
- Manages redeployment of network assets.
- Includes software modules for COOP.
- Plans operations generation, distribution, reconfiguration, and time synchronization.

System Administration

B-35. The system administrator can initialize, configure, monitor, and shut down the ISYSCON node. These activities are categorized into administration of the node hardware components, communications with the WAN, and administration of the data that is resident in the ISYSCON node. The system administrator assigns each AOR an ISYSCON node as its primary node. It then configures ISYSCON to support the requirements of the AOR.

Wide Area Network Manager

B-36. A WAN manager platform is present within each security domain (NIPR and SIPR). The WAN manager provides monitoring and control capabilities that report on the condition of the routers and network components. In addition, the WAN manager platform provides the capability to build and save Cisco device configurations (router and firewall) based upon mission specific criteria. Remote management capability exists using a standard Web browser. The JNN WAN manager platform is a Panasonic Toughbook laptop computer with the following software installed: Hewlett Packard OpenView Network Node Manager, Ciscoworks for Small Network Management Systems, Resource Manager Essentials 3.3, and CiscoView 5.3 components.

Hewlett Packard OpenView

B-37. The Hewlett Packard OpenView network node manger collects topology, trend, and event data that are used to troubleshoot report on, and analyze the network. It gives the network managers the information they need to ensure network availability and reliability.

B-38. Most devices within the JNN can be remotely accessed via the terminal server or KVM switch, with the use of a Web browser or HyperTerminal connection. There are some devices that cannot be accessed via the aforementioned means and require a manual man or machine interface. These devices include:

- SIPR and NIPR 100BTX/FX converters and hubs.
- Quad-MUX.
- All patch panels.
- KIV-19.

- KIV-7HS.

INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE

B-39. The systems addressed in this section are designed to provide IA/CND functions to the force.

INTRUSION DETECTION SYSTEMS

B-40. Internet Security Systems RealSecure IDS components monitor network and server activity for malicious intent or activity such as denial of service attacks, unauthorized access attempts, and pre-attack reconnaissance. When Internet Security Systems RealSecure IDS detects such activity, it can respond by recording the event, notifying the network administrator, terminating the attack, reconfiguring the firewall, and suspending or disabling an account.

ELECTRONIC KEY MANAGEMENT SYSTEM

B-41. Electronic Key Management System (EKMS) is a four tiered system. EKMS defines an overall key management system in support of the GIG. EKMS provides the capability for generation, distribution, destruction, and management of electronic key, as well as management of physical key and non-key COMSEC related items. EKMS provides functions that allow COMSEC account registration, privilege management, ordering, distribution, and accounting to direct the management and distribution of physical and electronic COMSEC materiel for the services. Other key features are:

- The Local Management Device/Key Processor (LMD/KP) supports the functions performed by the COMSEC Account Manager at the COMSEC account level of the EKMS structure. The LMD/KP is the workstation component at the COMSEC account level. It automates and computerizes many of the COMSEC procedures that have traditionally been performed manually within a COMSEC account. is the of the Electronic Key Management The Local Management Device/Key Processor provides the system management and audit support required to manage a COMSEC account.
- Local COMSEC Management Software (LCMS) is the NSA developed software that resides on an LMD/KP. It provides ordering, generation, distribution, and accounting for keying material (electronic or physical) and other associated COMSEC material. .
- Automated Communications Engineering Software (ACES) is a Windows NT-based software package loaded on a Panasonic CF-27 laptop. It is a planning and management tool that provides the load sets (keying materiel, hop sets) for single-channel radio systems. ACES automates the configuration of cryptographic devices and plans, manages, validates, generates, and distributes products associated with signal operating instructions and electronic protection.
- The Army Key Management System is an automated system designed for use in the tactical environments. It integrates the functions of COMSEC key management, control and distribution frequency management and signal operating instructions preparation.

ARMY INFORMATION SYSTEM

B-42. The Army information system provides firewall capabilities for the different ABCS platforms residing on the LAN. The Army information system hosts the common service capabilities for the ABCS 6.4 capable systems on the LAN. It primarily serves as a publish-and-subscribe server, coordinating the information produced by individual ABCS enabled platforms. Through a global positioning systems connection, it provides timing to the ABCSs resident on the LAN.

NORTON FIREWALL MANAGEMENT

B-43. Whether an organization deploys a single gateway or thousands, Symantec Enterprise Firewall offers a range of management tools to help reduce on-going operating costs. It provides scalable and centralized

management. Symantec Enterprise Firewall can be managed by the standalone, secure, Web-based Security Gateway Management Interface. For advanced management capabilities, the optional Symantec Advanced Manager and Symantec Event Manager for Security Gateway plugs in to the Symantec management console, therefore providing centralized policy CM, logging, alerting, and reporting for all security functions. The Symantec Advanced Manager and Symantec Event Manager provide secure, centralized, Web-based management of hundreds or thousands of security gateway deployments.

BLACKICE SERVER PROTECTION

B-44. BlackICE Server Protection (personal firewall) intrusion detection capabilities automatically detect and block malicious activities by monitoring all inbound and outbound traffic passing through the server. Users are instantly alerted of an attack and can easily identify the source and the method being used. Once an attempt is detected, BlackICE Server Protection automatically blocks traffic from that source so that the intruder is no longer a threat. BlackICE Server Protection also provides exhaustive reporting for common attacks on servers.

INFORMATION DISSEMINATION MANAGEMENT/CONTENT STAGING

INFORMATION DISSEMINATION MANAGEMENT-TACTICAL

B-45. IDM-T (SharePoint Portal, SQL Server 2000, iOra) is a system that provides a set of Web-based management tools for locating, transporting, and storing information products that meet the commander's critical information requirements. IDM-T is a combination of commercial off-the-shelf and government off-the-shelf products that include Microsoft Sharepoint Portal Server 2003, Server 2003, SQL Server 2000, SQL Server SP 3A, and iOra Software (not currently resident in all units, specifically the 3ID). IDM-T government off-the-shelf products include Web parts that include the following: request for information suite, briefing builder for battlefield update briefings, configurable clocks (time zone and count down banners), and commander's status board features.

B-46. Microsoft SharePoint Portal Server 2003 provides an enterprise business solution that integrates information from various systems into one solution, through single sign-on and enterprise application integration capabilities, with flexible deployment options and management tools. The portal facilitates end-to-end collaboration by enabling aggregation, organization, and search capabilities for people, teams, and information. Users can find relevant information quickly through customization and personalization of portal content and layout, as well as by audience targeting. Organizations can target information, programs and updates to audiences based on their organizational role, team membership, interest, security group, or any other defined membership criteria.

B-47. The SQL Server 2003 provides the enterprise data management platform to adapt in a fast-changing environment. It is benchmarked for scalability, speed, and performance. The SQL Server 2003 is a fully enterprise-class database product that provides core support for eXtensible Markup Language and Internet queries.

B-48. iOra for Microsoft SharePoint (not currently resident in all units, specifically the 3ID) is a collaboration tool that enables mobile use of SharePoint Portal capabilities by enabling users to browse and access the same Microsoft SharePoint content and functionality both online and offline. This software avoids dead links and ensures that integrated document management is constantly active.

B-49. Microsoft Exchange Server 2003 is messaging software that runs on servers and enables users to exchange individual and organizational e-mail and other forms of interactive communication through computer networks. Designed to interoperate with a software client application such as Microsoft Outlook and the Defense Message System User Agent (client software), Exchange Server also interoperates with Outlook Express and other e-mail client applications.

B-50. The Army information system hosts the common service capabilities for the ABCS resident on the LAN. It primarily serves as a publish-and-subscribe server, coordinating the information produced by individual ABCS platforms. Through the use of a global positioning system connection, the Army information system also provides timing to the different ABCS platforms resident on the LAN.

B-51. The SUN ONE server is used in conjunction with integrated battle command picture/publish-and-subscribe server services. It controls Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol/Secure (HTTPS) access to the publish-and-subscribe server portal.

B-52. The TOMCAT Server is a credentialing mechanism used in the Army information system server. It grants access to the global command and control system administration log tool (GSALT) once certificates have been verified. It also verifies all incoming connections for a security DOD root certificate.

B-53. The GSALT Server is a global command and control system administration log tool. It provides authentication and credential services through the GSALT administrative application. It is used in conjunction with TOMCAT to access command and control registry data. Services must be running to access the GSALT administrative console. The GSALT administrative console is used to give publishing privileges to open topics for the individual warfighting functions that will be connected to the Army information system.

B-54. The Integrated Battle Command Picture/publish-and-subscribe server provides the publish-and-subscribe server portal. It is used to create topics, and controls data flowing in and out of the Army information system server.

B-55. The command and control registry is administered by the command and control registry planner. It provides the common means of managing the address information that is vital to military messaging. It also allows a user to determine the unit reference number, IP address, host name, and other address data of a particular platform or unit. The command and control registry synchronizes this data across ABCSs so that all systems have the same addressing information. These capabilities support the configuration of the ABCSs.

B-56. State management provides a means by which elements of the ABCS network have the most current information. The data consists mainly of warning orders, OPORDs, FRAGOs, and unit task reorganizations.

Appendix C

Tactical Network Operations Scenarios

This appendix provides examples of the process flows for various NETOPS activities that may occur in the tactical environment. It will focus on familiar examples from known problem areas within the framework of Chapter 5.

OVERVIEW

C-1. Below are some general guidelines that are followed during the development of the scenarios referenced throughout this appendix:

- Follow the operational models previously established in Chapter 5.
- Remain consistent with the AENIA, joint and Army NETOPS CONOPS, etc.
- Establish best practices consistent with the proper tradeoff between commercial best practices versus tactically unique requirements. Solid rationale is presented for deviations from commercial best practices.

C-2. The intent is that signal Soldiers in the field will be able to use these scenarios to understand the operational context and employment of the NETOPS activity under question.

C-3. These processes are depicted in a business process diagram using the business process modeling notation (BPMN) version 1.0 specification. The BPMN 1.0 specification (BPMN, May 2004) provides a detailed and useful definition: The BPMN specification provides a graphical notation for expressing business processes in a business process diagram. The objective of BPMN is to support business process management by both technical users and business users. This objective is achieved by providing a notation that is intuitive to business users yet able to represent complex process semantics. The BPMN specification also provides a mapping between the graphics of the notation and the underlying constructs of execution languages, particularly business process execution language for Web services.

C-4. Several symbols are used in the business process diagrams that should be described for clarity. Figure C-1 and C-2 serve as a legend for the business process diagrams contained within this section.

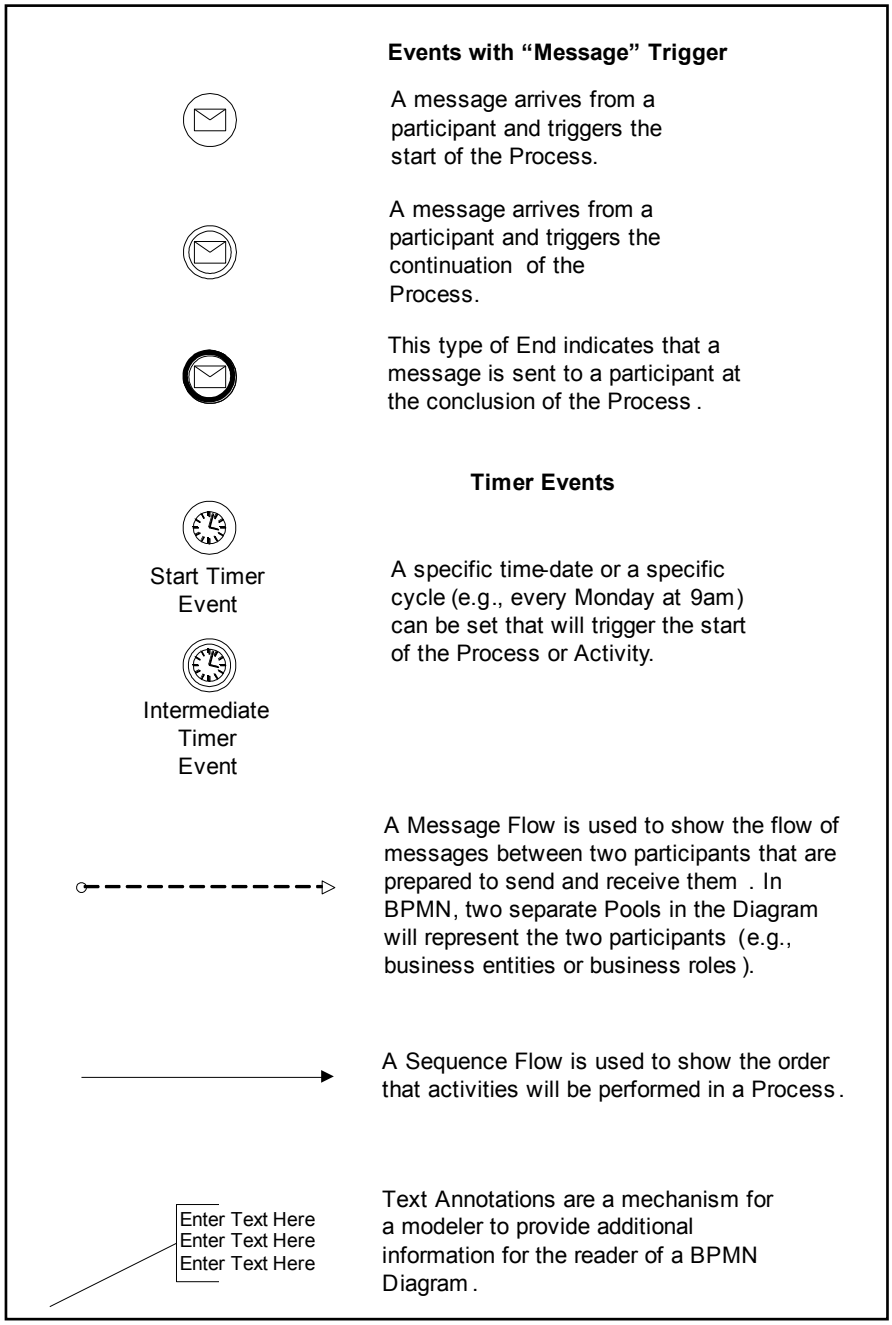

Figure C-1. BPMN flow and connection elements

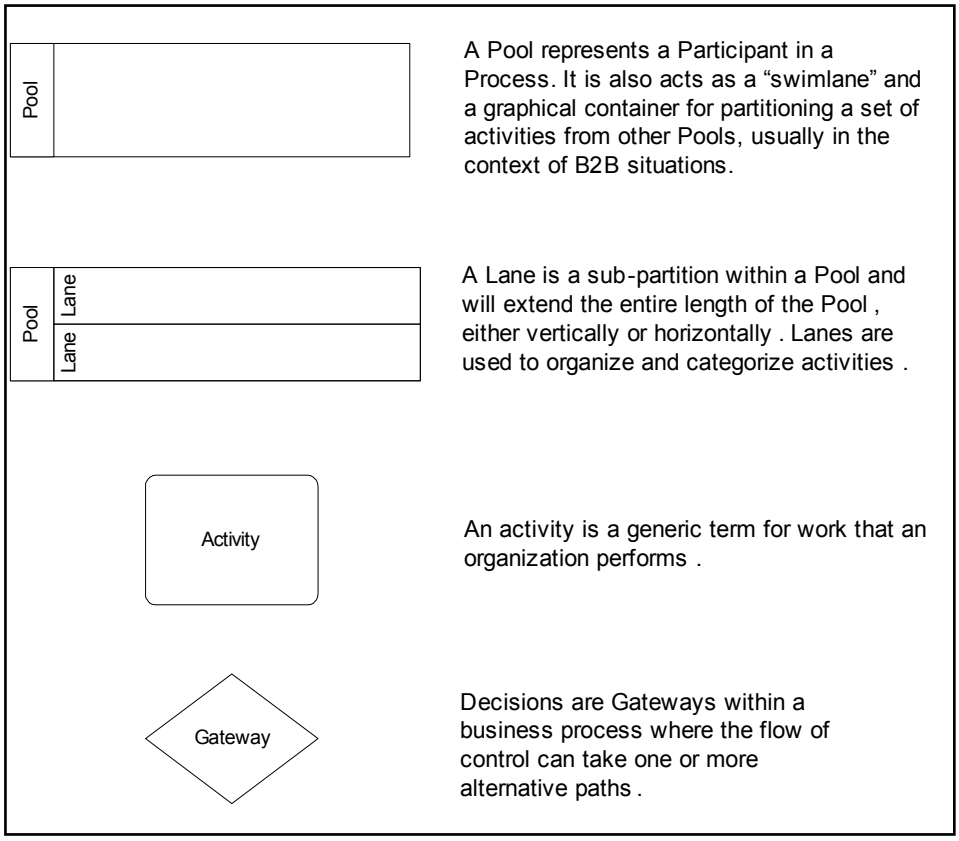

Figure C-2. BPMN core elements

NON-GLOBAL CONFIGURATION MANAGEMENT AND CHANGE MANAGEMENT SCENARIO

C-5. The following scenario explains the activities involved in implementing a configuration change on a network device within the Army's enterprise. This configuration change is considered non-global, as it requires a change to be made only at a single battalion level within the Army enterprise. When a configuration change is required that affects devices across the Army enterprise, it is then considered a global configuration change. A scenario illustrating a global configuration change is provided in the next section.

C-6. Although the narrative for this scenario focuses on implementing a change to the configuration on a port of a firewall, it details the activities associated with the change management process in general; therefore, it is applicable to implementing any type of non-global change within the theater enterprise.

C-7. The process flow depicted in Figure C-3 describes the actions taken by various organizations within the tactical echelons, residing in an Army theater, as they react to a new application being added to support a battalion command post's mission.

C-8. It is important to note that NETOPS activities rely on one another in order to complete a process. To emphasize this fact, portions of related NETOPS activities are included in this scenario's diagram in addition to change management activities. The scenario in Figure C-3 begins with the incident and problem management activity. It should be noted that the incident and problem management activity has been abbreviated in this scenario for the purpose of simplicity. The change management activity can be found in the incident and problem management activity which begins in Step 10 of the scenario. The change management activity continues through Step 15 and provides the mechanism in which an orderly and coordinated change is implemented to the firewall's port configuration. CM is also an integral activity of this scenario. It is initiated as a result of the change management activity and occurs in Steps 14 through 16

(some of the steps in the scenario apply to more than one activity). CM ensures that the new configuration of the firewall is documented and made available to all interested organizations.

ASSUMPTIONS

C-9. This scenario assumes that there is a pre-established firewall configuration change policy in effect at the theater. It also assumes that the standard configuration policy for the theater's firewalls specifies deny all and permit by exception and that the port to be changed on the battalion's firewall is associated with a theater-approved application.

C-10. This scenario also assumes that the division has the final authority to approve the configuration change in question given that the firewall is an echelon-above-brigade managed system. The ARFOR NOSC is not required to approve the change unless otherwise directed, but notification of the change is required.

C-11. This scenario further assumes that a configuration database system is in operation within the theater, which facilitates the viewing of all configuration changes for all organizations.

SCENARIO NARRATIVE

C-12. This scenario begins with a new application being added to support a battalion command post mission. Since the application was not resident in the battalion command post at the onset of operations, deny all and permit by exception protocol results in the application's communication port being blocked at the local firewall. The designations G-6 and S-6 refer to both the individual and staff. The following are step-by-step instructions for the scenario—

Step 1: The battalion S-6 receives a message from a user on the battalion network stating that a newly installed application is not functioning properly.

Step 2: The battalion S-6 investigates the problem, but cannot determine the cause. If the cause of the problem can be determined and corrective action is authorized, then the process proceeds to Step 18.

Step 3: The battalion S-6 notifies the BCT S-6 of the problem.

Step 4: The BCT S-6 directs the brigade signal company to investigate the problem.

Step 5: The BCT signal company collaborates with the battalion S-6 to troubleshoot the problem, but cannot determine the cause.

Step 6: The BCT S-6 notifies the G-6 of the problem.

Step 7: The G-6 directs the Warfighter Integration and Support Cell (WISC) to investigate the problem.

Step 8: The WISC collaborates with the BCT signal company and the battalion S-6 to investigate and identify the cause of the problem (a blocked port on the battalion command post's firewall). Since the problem was identified by the WISC, it should be noted that the ARFOR and TNOSC do not get involved in the troubleshooting process.

Step 9: The WISC notifies the G-6, the BCT S-6, and the battalion S-6 of the cause of the problem.

Step 10: The battalion S-6 submits a firewall port configuration request for change to the BCT S-6 to have the blocked port opened.

Step 11: The BCT S-6 receives, validates, and forwards the firewall port configuration request for change to the G-6.

Step 12: The division G-6 receives and approves the firewall port configuration request for change.

Step 13: The division G-6 directs the WISC to schedule the firewall port configuration change.

Step 14: The WISC consults the G-6, BCT S-6, and battalion S-6 for an available execution window, schedules the firewall port configuration change, and notifies the G-6, the BCT S-6, and the battalion S-6 of the schedule.

Step 15: At the scheduled time, the WISC executes the firewall port configuration change.

Step 16: The WISC updates the configuration database and notifies the ARFOR NOSC, the TNOSC, the G-6, the BCT S-6, and the battalion S-6 that the change has been executed.

Step 17: The battalion S-6 verifies that the application is now functional (if it is not functional, then the process begins again from Step 2).

Step 18: The process ends when the battalion S-6 verifies that the application is functional.

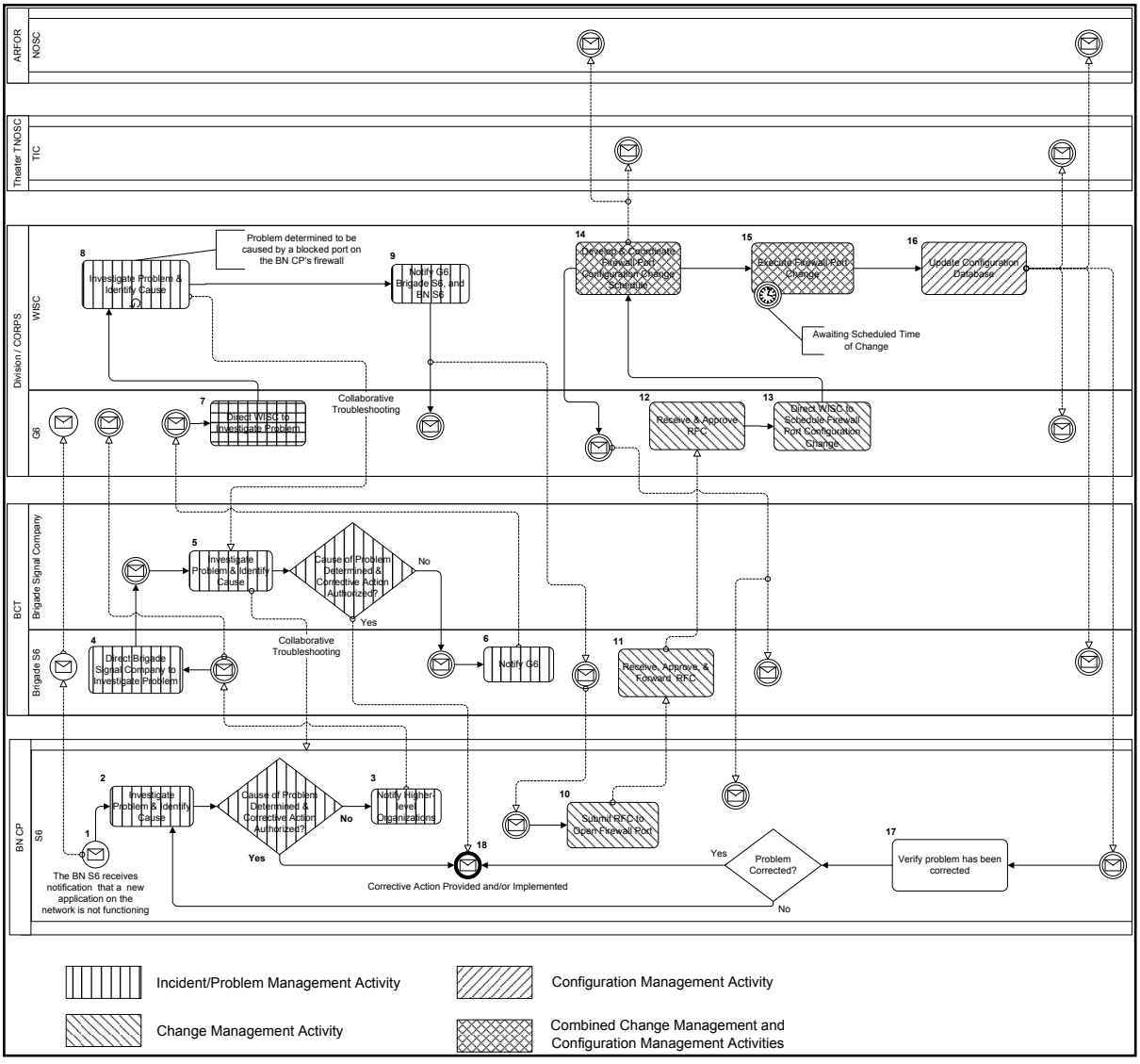

Figure C-3. Non-global configuration change scenario

GLOBAL CONFIGURATION CHANGE SCENARIO

C-13. The following scenario illustrates the activities involved in implementing a change on a network device within the Army's enterprise. This change is considered global, as it requires a change to be made to all devices within the Army enterprise. When a change is required that only affects devices within a small portion of the Army enterprise it is then considered a non-global change. A scenario illustrating a non-global change is also provided above.

C-14. Although the narrative for this scenario focuses on implementing a change to the ACL configuration of the theater's routers, it details the activities associated with the change management process in general; therefore, it is applicable to implementing any type of global change within the theater enterprise.

C-15. The process flow depicted in Figure C-4 illustrates the actions taken by various organizations, within the theater and Army level echelons, as they react to a directive from the A2TOC to change the ACL configurations on all Army routers within the theater.

C-16. As stated earlier, NETOPS activities are interdependent. This scenario involves the CM activity in addition to change management. The change management activity occurs in Steps 1 through 7.1. This activity is initiated as the result of the A2TOC directing a global change to all Army routers' configurations. It also provides the mechanism in which an orderly and coordinated change is implemented. CM is also an integral activity in this scenario. It is initiated as a result of the change management activity and occurs in Step 7, 7.1, and 8 in the scenario (some of the steps in the scenario apply to more than one activity). CM ensures that the new configuration of the Army routers is documented and made available to all interested organizations.

ASSUMPTIONS

C-17. This scenario assumes that there is a pre-established router ACL configuration change policy in effect in the theater. This scenario further assumes that because the change originated from the A2TOC the ARFOR NOSC is required to approve such a change. It is also assumed that the ARFOR NOSC will approve the change.

C-18. In addition, this scenario assumes that a configuration database system is in operation within the theater, which then facilitates the viewing of all configuration changes for all organizations.

SCENARIO NARRATIVE

C-19. This scenario in Figure C-4 is triggered by a notification to the TNOSC from the A2TOC that an Army-wide change to router ACL configurations must be implemented throughout the theater. The following is a step-by-step explanation for the scenario—

Step 1: The TNOSC receives notification from the A2TOC that the ACL configurations on all Army routers within the theater must be changed.

Step 2: The TNOSC notifies the ARFOR NOSC of the ACL change criteria and requests approval to initiate the implementation of the change. If the ARFOR NOSC approves the change, then the process continues with Step 3. If the ARFOR NOSC does not approve the change, then the process continues with Step 3.1.

Step 3: Upon approval, the TNOSC disseminates the ACL change criteria to the G-6 at the division.

Step 3.1: Upon non-approval, the TNOSC notifies the A2TOC that the change is not approved by the ARFOR NOSC and requests further direction. At this point, the process ends, and the A2TOC and the ARFOR NOSC address the issue of the ACL configuration change approval.

Step 4: Upon notification from the TNOSC of the ACL configuration change, the G-6 directs the WISC to schedule the ACL configuration change.

Step 5: The WISC develops and coordinates a schedule for the ACL configuration change. The schedule is provided to ARFOR NOSC, the A2TOC, the TNOSC, the G-6, the BCT S-6, and the battalion S-6. Upon notification from the TNOSC of the ACL configuration change, the ARFOR NOSC develops and coordinates a schedule for the ACL configuration change. The schedule is provided to all corps and above Army networks and any expeditionary BCTs within the ARFOR AOR.

Step 6: The WISC, ICW each vested organization, implements the ACL configuration change for the division AOR. At the prescribed time, the ARFOR NOSC, ICW each vested organization, implements the ACL configuration change for all echelon above corps Army networks and any expeditionary BCTs within the ARFOR AOR.

Step 7: The WISC notifies each vested organization that the change has been executed. It should be noted that if the change has any adverse effects, then the incident and problem management process described next will be initiated.

Step 7.1: The process ends with the ARFOR NOSC notifying each vested organization that the change has been executed. It should be noted that if the change has any adverse effects, then the incident and problem management process described in the next section will be initiated.

Step 8: Upon notification that directed changes have been made, the A2TOC updates the configuration database.

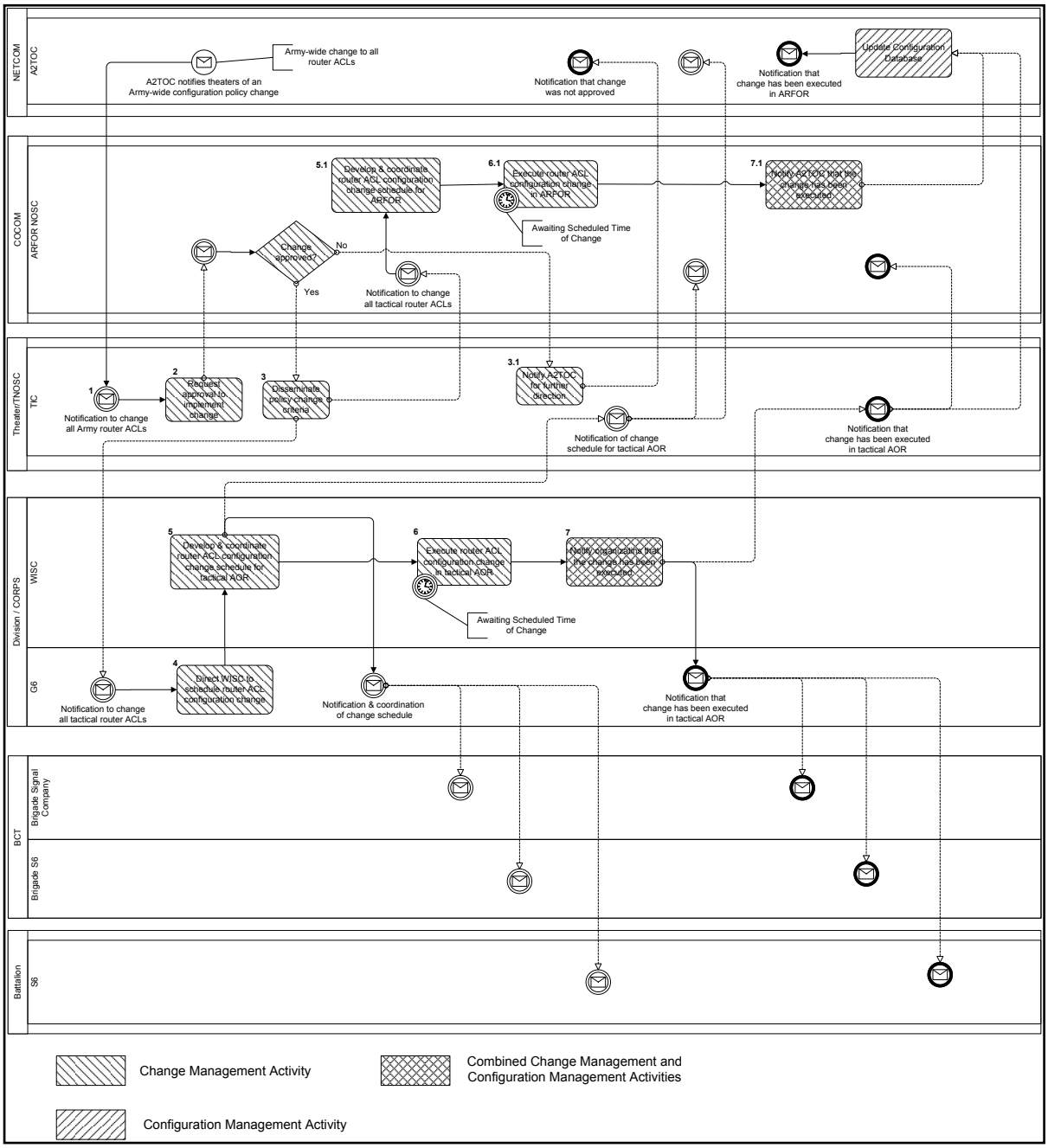

Figure C-4. Global configuration change scenario

INCIDENT AND PROBLEM MANAGEMENT SCENARIO

C-20. The process flow depicted in Figure C-5 describes the actions taken by various organizations, within the echelons residing in an Army theater, as they react to a capability-related incident and problem and the ensuing trouble ticket.

C-21. The following scenario works through the activities involved in managing a capability-related incident or problem. This scenario illustrates a situation where there is a problem at the battalion level and the problem is escalated all the way to the TNOSC, if necessary, to resolve the issue. It is the responsibility

of the ARFOR NOSC to involve the TNOSC if the ARFOR NOSC is unable to resolve the problem on its own.

C-22. Although this scenario focuses on the processing of incidents or problems related to capabilities, it is also applicable to processing any type of incident or problem within the enterprise.

C-23. As stated earlier, NETOPS activities are interdependent. This scenario involves both the change management and CM activities in addition to incident and problem management. The incident and problem management activity occurs when the battalion S-6 opens a trouble ticket concerning a capability that has been reported by a battalion subscriber. When the battalion S-6, signal company, WISC, ARFOR NOSC, or TIC determines the cause of the problem and performs corrective actions (Steps 4.1, 7.1, 10.1, 12.1, and 14.1, respectively), these steps involve the incident and problem management activity as well as the change management and CM activities. In performing corrective actions, some type of change will eventually be made to a system or the network. At this time, the change management activity is initiated. This activity provides the mechanism in which an orderly and coordinated change is implemented. The change management activity will normally result in some type of configuration change. The resulting configuration change will initiate the CM activity in which the altered configuration will be documented. This will ensure that the new configuration, resulting from correcting an incident or problem, is documented and made available to all organizations.

ASSUMPTIONS

C-24. This scenario assumes that a customer relationship management system is in operation within the theater, which facilitates the notification of capability-related incidents and problems to the responsible organizations. It is also assumed that the customer relationship management system facilitates the processing of trouble tickets related to incidents and problems. Consequently, each organization within the theater is capable of viewing each trouble ticket through its lifecycle.

C-25. This scenario also assumes that the theater maintains a knowledge base that is available to each organization in the theater that contains historical data related to past problems, their causes, and their resolutions.

Scenario Narrative

C-26. This scenario is depicted in Figure C-5. The process is triggered by a notification to the battalion S-6 from a local subscriber that a capability is not functioning. The following is a step-by-step explanation for the scenario—

Step 1: A battalion subscriber notifies the battalion S-6 that a capability is not functioning.

Step 2: The battalion S-6 opens a trouble ticket for the unknown problem. Note that through the customer relationship management system, all organizations are capable of viewing the trouble ticket. The BCT S-6 tracks the trouble ticket and alerts the BCT signal company that their services may be required to resolve the problem. Similarly, the G-6 tracks the trouble ticket and alerts the WISC that their services may be required to resolve the problem. The TNOSC and ARFOR NOSC also track the trouble ticket.

Step 3: The battalion S-6 queries the theater's knowledge base to determine if the problem has been encountered previously and, if so, what corrective action was taken. If the problem is not found in the theater's knowledge base, then the process continues with Step 4. If the problem is found in the theater's knowledge base, then it is re-categorized as an incident and the process continues with Step 4.1.

Step 4: The battalion S-6 collaborates with the battalion subscriber and investigates the problem. If the cause of the problem is determined and the corrective action is authorized, then the process continues to Step 4.1. If the problem cannot be determined or the corrective action is not authorized, then the process continues to Step 5.

Step 4.1: Throughout the change management activity, the battalion S-6 instigates corrective actions for the problem and the process continues to Step 4.2.

Step 4.2: Upon completion of corrective actions, the battalion S-6 updates and closes the trouble ticket and documents any configuration changes. The process then continues to Step 15.

Step 5: The battalion S-6 updates the trouble ticket and escalates it to the BCT, and the process continues to Step 6. It is important to note that the BCT S-6 and BCT signal company are capable of viewing the updated trouble ticket.

Step 6: The BCT S-6 directs the BCT signal company to investigate the problem.

Step 7: The BCT signal company collaborate with the battalion S-6 and the battalion subscriber to investigate the problem. If the cause of the problem is determined and the corrective action is authorized, then the process continues to Step 7.1. If the problem cannot be determined or the corrective action is not authorized, then the process continues to Step 8.

Step 7.1: Through the change management activity, the BCT signal company instigate corrective actions for the problem and the process continues to Step 7.2.

Step 7.2: Upon completion of corrective actions, the BCT signal company update and close the trouble ticket and record any configuration changes. The process then continues to Step 15.

Step 8: The BCT signal company updates the trouble ticket and the BCT S-6 escalates it to the division. The process then continues to Step 9. It is important to note that both the G-6 and the WISC are capable of viewing the updated trouble ticket.

Step 9: The G-6 directs the WISC to investigate the problem.

Step 10: The WISC collaborates with the BCT S-6, the battalion S-6, and the battalion subscriber to investigate the problem. If the cause of the problem is determined, then the process continues to Step 10.1. If the problem cannot be determined the process continues to Step 11.

Step 10.1: Throughout the change management activity, the WISC instigates corrective actions for the problem and the process continues to Step 10.2.

Step 10.2: Upon completion of corrective actions, the WISC updates and closes the trouble ticket and documents any configuration changes. The process then continues to Step 15.

Step 11: The WISC updates the trouble ticket and escalates it to the ARFOR NOSC and the process continues to Step 12.

Step 12: The ARFOR NOSC collaborates with the WISC, the BCT S-6, battalion S-6, and battalion subscriber to investigate the problem. If the cause of the problem is determined, then the process continues to Step 12.1. If the problem cannot be determined, then the process continues to Step 13.

Step 12.1: Through the change management activity, the ARFOR NOSC instigates corrective actions for the problem and the process continues to Step 12.2.

Step 12.2: Upon completion of corrective actions, the ARFOR NOSC updates and closes the trouble ticket and documents any configuration changes. The process then continues to Step 15.

Step 13: The ARFOR NOSC updates the trouble ticket and escalates it to the TNOSC and the process continues to Step 14.

Step 14: The TNOSC collaborates with the ARFOR NOSC, the WISC, the BCT S-6, the battalion S-6, and the battalion subscriber to investigate the problem. If the cause of the problem is determined, then the process continues to Step 14.1. If the cause of the problem is not identified, the TNOSC will consult subject matter experts, vendors, or other sources until the problem is resolved. Then the process will continue with Step 14.1.

Step 14.1: Through the change management activity, the TNOSC performs corrective actions for the problem and the process continues to Step 14.2.

Step 14.2: Upon completion of corrective actions, the TNOSC updates and closes the trouble ticket and documents any configuration changes. The process then continues to Step 15.

Step 15: Upon notification of the closed trouble ticket, the TNOSC updates the theater's knowledge base with the corrective actions taken to resolve the problem. It is important to

note that through the customer relationship management system, all echelons and their organizations are notified of the trouble ticket closure.

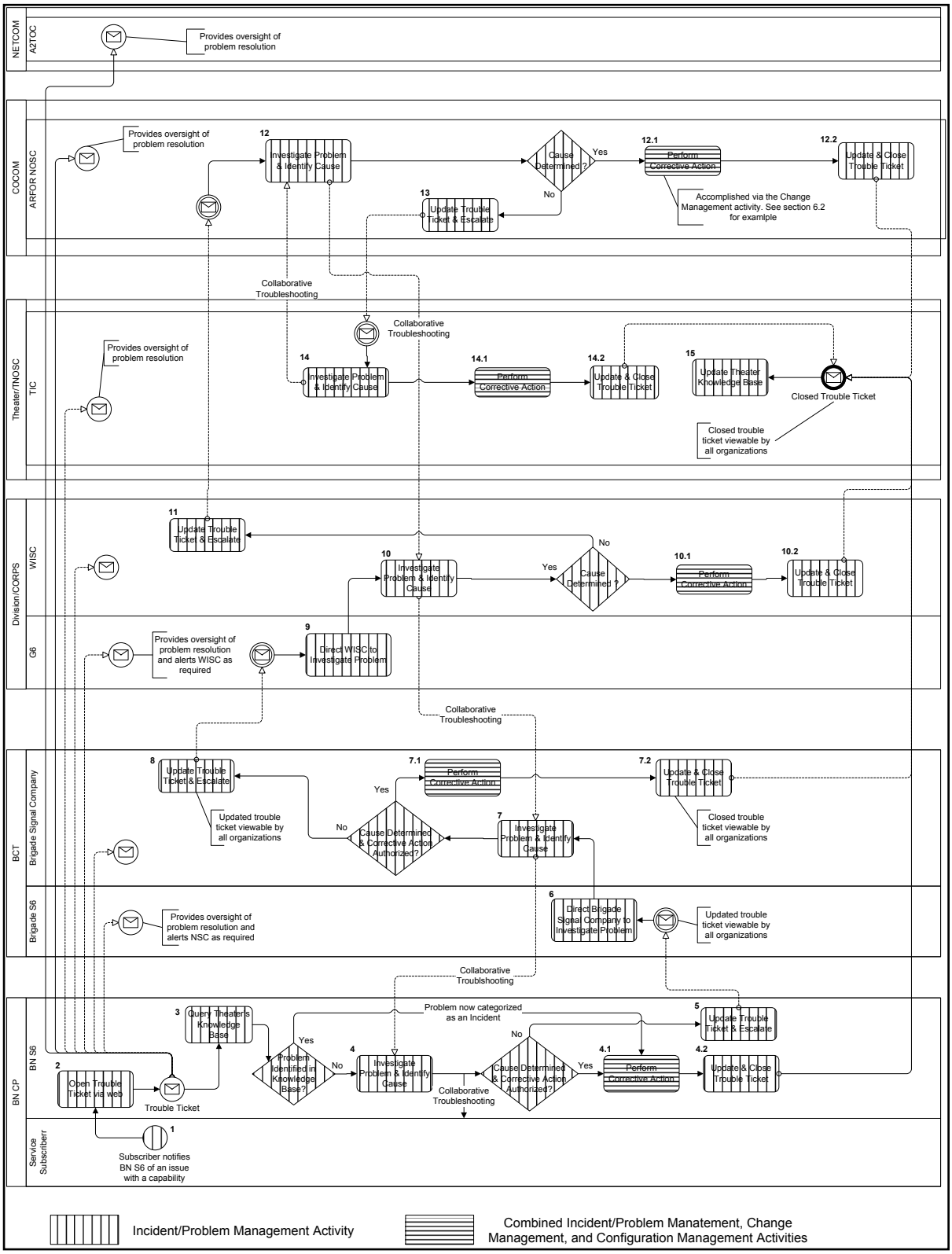

Figure C-5. Incident and problem management scenario

POLICY MANAGEMENT SCENARIO

C-27. The following scenario works through the activities involved in implementing and managing a temporary exception to policy. Although the narrative for this scenario focuses on the temporary exception to border routing policy, it details the activities associated with policy management in general. Therefore, it is applicable to managing any type of Army tactical policy.

C-28. The process flow depicted in Figure C-6 describes the actions taken by various organizations, within the tactical echelons residing in an Army theater, as they identify and process a temporary exception to BCT border router policy.

ASSUMPTIONS

C-29. This scenario assumes that there is a pre-established BCT border router configuration policy in effect. It is further assumed that the standard configuration policy for the BCT border routers specifies that no redistribution of foreign routes is allowed into the Border Gateway Protocol process.

Scenario Narrative

C-30. This scenario is depicted in Figure C-6. The scenario begins when the BCT is tasked to support a non-organic group of networks. The following is a step-by-step explanation for the scenario—

Step 1: During the course of a mission, the BCT is tasked to support a non-organic group of networks. To support this task, the BCT identifies a need for a temporary exception to policy regarding border router redistribution. Throughout the change management activity, the BCT S-6 sends a request for change requesting a temporary exception to policy. The request is sent to its commanding headquarters, which is currently a division, for review.

Step 2: The division G-6 analyzes the request, and if the division G-6 agrees that the request is valid, then the process continues with Step 3. If the division G-6 does not agree with the request, then the process continues with Step 3.1 and the scenario ends.

Step 3: The division G-6 determines if the temporary exception to policy request could have an adverse impact on the availability or security of networks external to the division and BCT. If possible, the process continues with the Step 4.1. If not, the scenario continues with Step 4.

Step 3.1: The division G-6 notifies the BCT S-6 that the temporary exception to policy has been rejected based upon possible mission ramifications. The division may suggest an alternate solution or instruct the BCT to operate as effectively as possible within the boundaries of Army policy.

Step 4: The division G-6 notifies the BCT that the temporary exception to policy has been approved. The division also notifies the ARFOR of the temporary exception to policy for informational purposes. ARFOR notifies its parent joint command and numbered Army TIC of the temporary exception to policy. The numbered Army TIC notifies other numbered Army components (e.g., SC[T]) and the A2TOC of the temporary exception to policy. The A2TOC then notifies the CIO G-6 and the US Army Signal Center of the temporary exception to policy. The activity then continues with Step 5.

Step 4.1: The division G-6 sends the temporary exception to policy request to its commanding headquarters, which is the ARFOR.

Step 4.2: The ARFOR analyzes the temporary exception to policy request. If the ARFOR determines that the temporary exception to policy is valid, then the process continues with Step 4.3. If the ARFOR determines that the temporary exception to policy is not valid, then the process continues with Step 4.3.1.

Step 4.3: The ARFOR determines if this temporary exception to policy could have an adverse impact on the availability or security of networks external to the ARFOR. If possible, the process continues with the next step.

Step 4.3.1: The ARFOR notifies the division G-6 that the temporary exception to policy has been rejected based upon possible mission ramifications. ARFOR may suggest an alternate solution or instruct the BCT to operate as effectively as possible within the boundaries of Army policy. The scenario then returns to Step 3.1.

Step 4.4: The ARFOR notifies the division G-6 that the temporary exception to policy has been approved. The process returns to Step 4.

Step 4.4.1: Processing for the temporary exception to policy request is forwarded to the ARFOR's joint headquarters. Activities are then dictated by joint policy and the scenario ends.

Step 5: Throughout the change management and CM activities, the BCT implements the temporary exception to policy. The scenario then continues with Step 6.

Step 6: Upon redeployment, the BCT, through the change management and CM activities, revokes the temporary exception to policy and reconfigures border routers to once again comply with permanent Army policy. During redeployment after action review, the BCT may identify a need to alter permanent Army policy regarding BCT border router configurations in order to capture lessons learned. The BCT submits this policy change proposal via the chain of command.

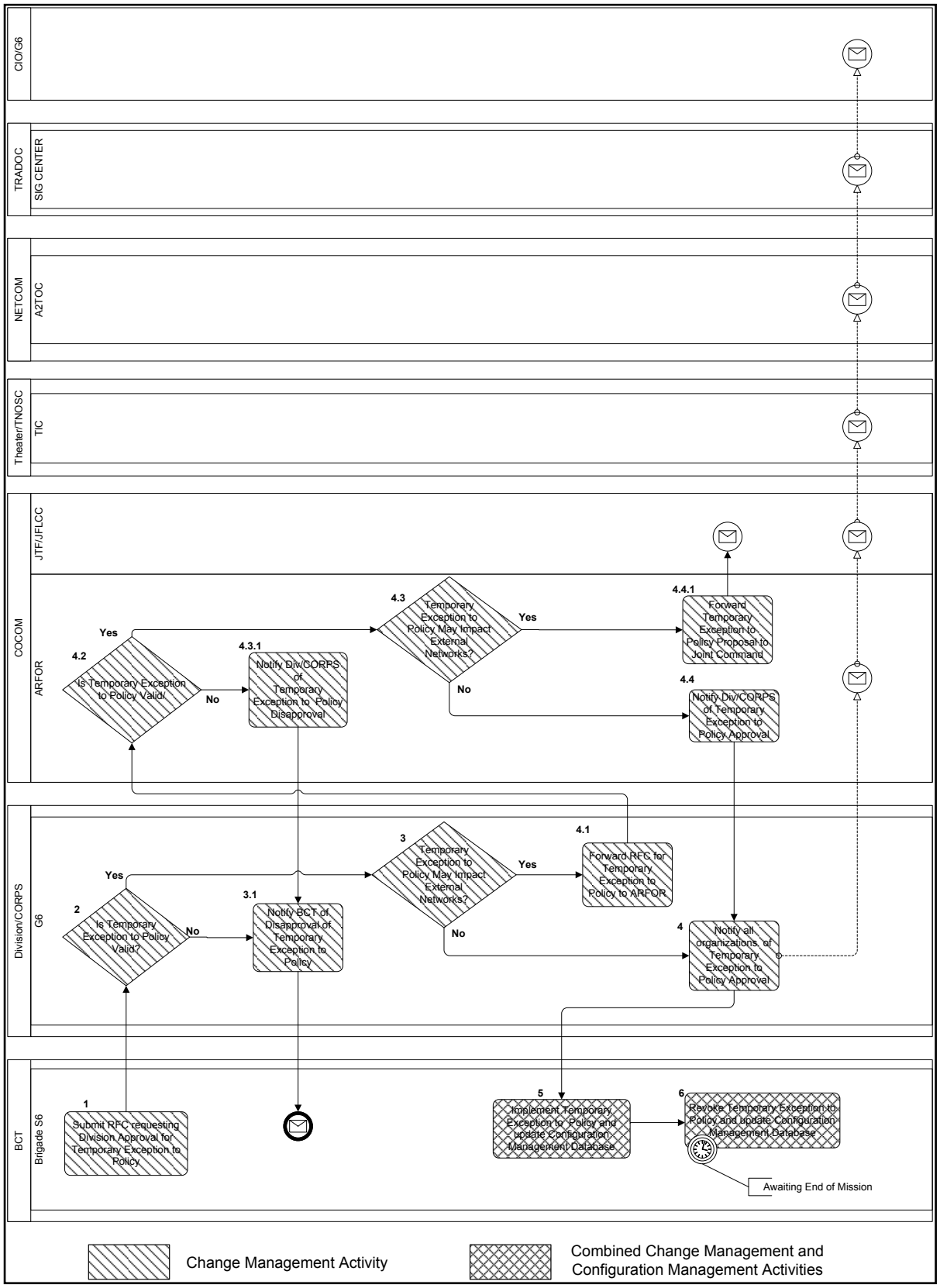

Figure C-6. Policy management scenario

NETWORK OPERATIONS SHARED SITUATIONAL AWARENESS SCENARIO

C-31. The following scenario works through the activities involved in developing and requesting theater NETOPS shared SA views.

C-32. The process flow depicted in Figure C-7 describes the actions taken by various organizations, within the tactical echelons residing in an Army theater, as they prepare systems to support the development of tailored theater NETOPS shared SA views by the TNOSC. The scenario also provides information concerning the process that is necessary to request tailored views, for various uses, at their echelon.

ASSUMPTIONS

C-33. This scenario assumes that the TNOSC plays a role in the infrastructure monitoring processes and NETOPS shared SA development for Army theaters down to the BCT level.

SCENARIO NARRATIVE

C-34. This scenario is depicted in Figure C-7. The following is a step-by-step explanation for the scenario—

Step 1: Army doctrine, policy, and guidance direct the development of a NETOPS shared SA for all missions given in any theater.

Step 2: TIC personnel will be responsible for ensuring the relevant tactical systems within the numbered Army and TNOSC AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC.

Step 3: Through the infrastructure monitoring processes, the TNOSC will begin to receive theater OPORD 05-01 NETOPS shared SA data.

Step 4: The TNOSC will store and normalize the theater NETOPS shared SA data.

Step 5: The TNOSC will develop an aggregated theater NETOPS shared SA view that is automatically forwarded to the A2TOC. The TNOSC will develop specific NETOPS shared SA views based on requests from theater consumer organizations.

Step 6: The A2TOC will automatically receive an aggregated theater NETOPS shared SA view from the TNOSC.

Step 7: The A2TOC will take all the aggregated theater NETOPS shared SA views from all Army theaters and produce an Army NETOPS shared SA view.

Step 8: Either prior to or upon entry to an Army theater, the BCT S-6 will direct the BCT signal company to equip and configure all relevant systems in the BCT AOR in order to report NETOPS shared SA data.

Step 8.1: The signal company personnel will be responsible for ensuring the relevant systems within the BCT AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC.

Step 9: Either prior to or upon entry to an Army theater, the division G-6 will direct the WISC to equip and configure all relevant systems in the division AOR in order to report NETOPS shared SA data.

Step 9.1: WISC personnel will be responsible for ensuring the relevant systems within the division AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC.

Step 10: Upon its instantiation as a joint operational area command, the ARFOR NOSC will be responsible for ensuring the relevant systems within the ARFOR AOR are equipped and configured to report OPORD 05-01 required NETOPS shared SA data to the TNOSC.

Step 11: At any time the BCT commander or BCT staff may need specific NETOPS shared SA views to ascertain the health of the NETOPS capabilities.

Step 11.1: The BCT S-6 will request appropriate NETOPS shared SA views from the TNOSC.

Step 11.2: The BCT S-6 will receive requested NETOPS shared SA views from the TNSOC.

Step 12: At any time the division commander or division staff may need specific NETOPS shared SA views to ascertain the health of the NETOPS capabilities.

Step 12.1: The division G-6 will request appropriate NETOPS shared SA views from the TNOSC.

Step 12.2: The division G-6 will receive requested NETOPS shared SA views from the TNOSC.

Step 13: At any time the CCDR, JTFs, JFLCCs, JNCCs, theater NETOPS centers, and TNCCs may require specific NETOPS shared SA views to quickly assess and react to capability degradations that impact, or have the potential to impact, its warfighting capability.

Step 13.1: The ARFOR NOSC will request the appropriate NETOPS shared SA views from the TNOSC.

Step 13.2: The ARFOR NOSC will receive requested NETOPS shared SA views from the TNOSC.

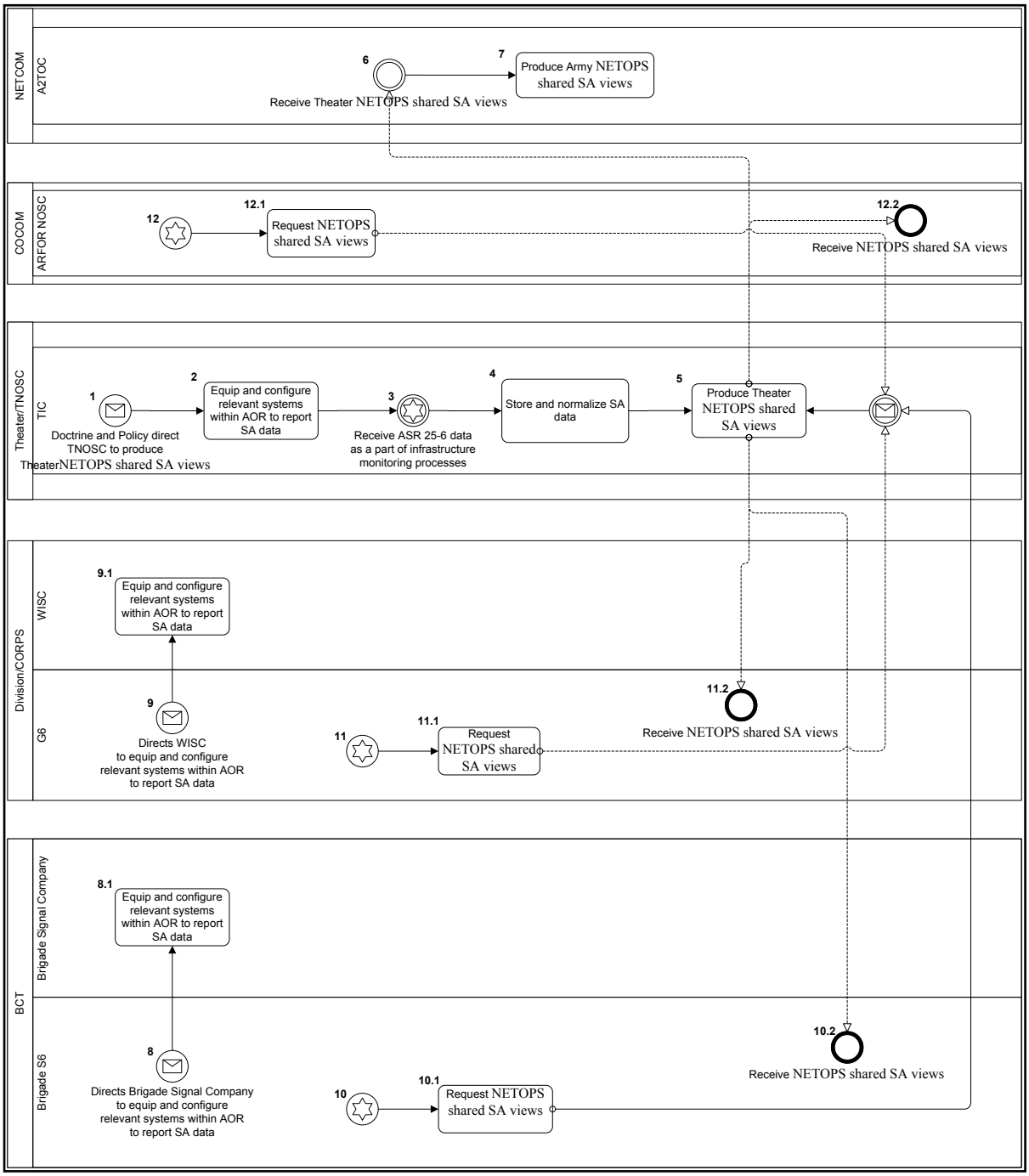

Figure C-7. NETOPS shared SA scenario

Appendix D

Network Management and Operations: Division

This appendix provides division commanders and staff members an understanding of systems and personnel that comprise the communications network at division and below. It also provides brief overviews of the related mission responsibilities of the division G-6, division signal company and the brigade and battalion level communications capabilities and responsibilities.

OVERVIEW

D-1. As the primary tactical and operational war fighting headquarters the division requires a robust command and control information network architecture supported by NETOPS personnel at division and below. The division is supported by organic G-6 section NETOPS (network management, IDM and IA) personnel and by the network transport personnel and assets within the division signal company. These personnel and assets install, operate, maintain, manage and defend the federations of networks. The federation of networks collectively enables joint and expeditionary battle command. The network enables leaders to command and control maneuver formations, sustain the force, and achieve broad political military objectives across the full spectrum of operations. It is an integrated entity and pervasive throughout the operational environment and touches every entity, to include the individual Soldier. The network as a critical weapon in the fight must be robust, redundant, flexible and adaptive to the commander.

DIVISION G-6

D-2. The division G-6 is the senior signal officer who exercises staff oversight of the division information network and has the level of experience to anticipate the need to dynamically change the network in support of the division commander's scheme of maneuver. The G-6 derives his authority to control the network from the division commander; this authority empowers him to utilize all signal equipment and personnel for the successful completion of his mission. The successful accomplishment of the mission implies that all signal training requirements are met prior to employment. The G-6 is accountable for all network transport, network services and the viability of information systems across the force. He controls these network assets via the NOSCs and utilizes the technical service order; much like the division G-3 uses the FRAGO to control the maneuver forces under the division.

D-3. The G-6 network responsibilities encompass all the management and control of the entire federation of networks. The NOSC enables the G-6 to monitor the health of the network in support of the command. The division G-6 is organized and resourced to provide NETOPS support to the division command posts (tactical [TAC], main, and mobile command group). The G-6 utilizes NETOPS functions to synchronize disparate division unit networks into one division information network, as a part of the LWN and GIG. It should be noted that the NETOPS functions performed in the subordinate support brigades and BCTs provide a second echelon of NETOPS management that the division G-6 coordinates as part of the greater NETOPS plan. Figure D-1 provides a recommended G-6 organization.

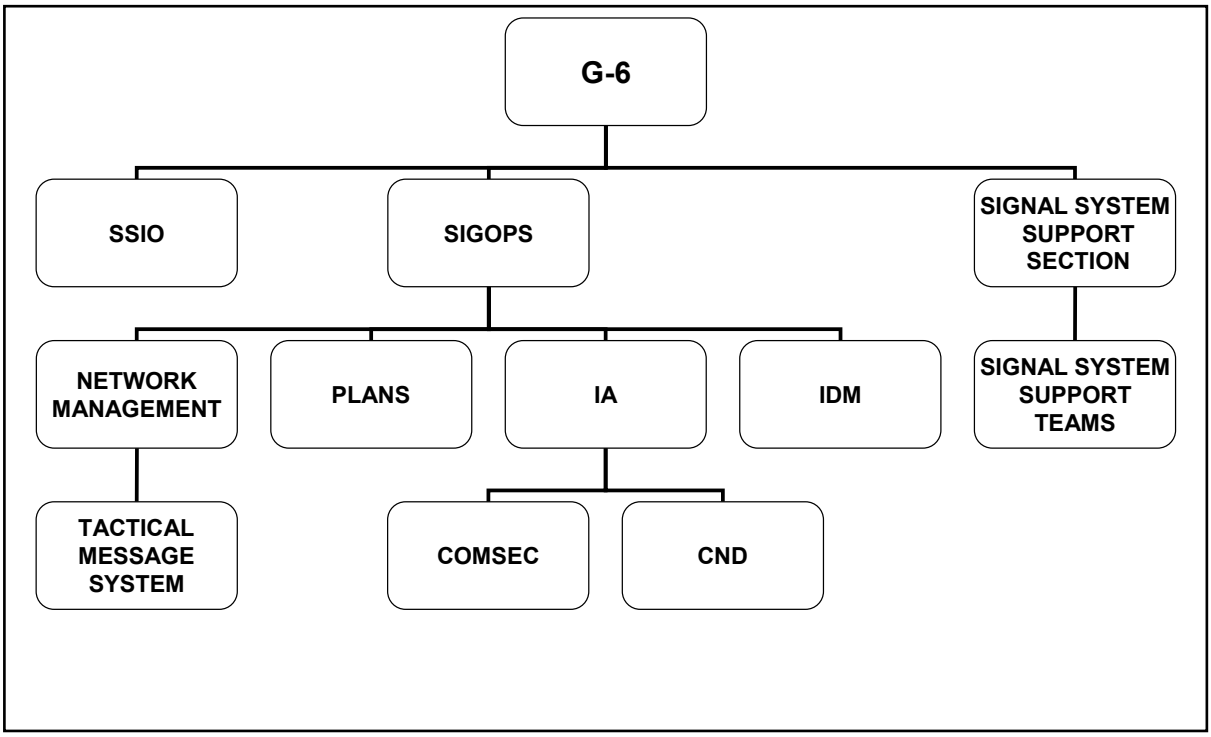

Figure D-1. G-6 section organization

DIVISION G-6 ORGANIZATION

D-4. **The G-6 Signal Operations (SIGOPS) Section**. The SIGOPS section consists of the NETOPS functions which includes the network management and the tactical message system cell, IDM, IA, CND, and COMSEC. In addition the SIGOPS section contains a NETOPS plans cell. The cells within the SIGOPS section performs the following functions:

- Integrates network management, IDM, and IA functions.
- Maintains network connectivity across the division, to include units deployed to the AOR, units en route to the AOR, and units at home station.
- Manages the division network from the applications residing on individual platforms through the points at which the division network connects to the LWN.
- Executes deliberate modifications to the division network in order to meet the needs of the commander.
- Manages requirements; accepts, validates and tracks headquarters and subordinate unit communication requirements (computers, cell phones, radios, etc.).
- Monitors network performance.
- Manages the quality of service of the services provided through the division network, including the interoperability of the division network with external networks that are not controlled by the G-6 (e.g., Global Broadcast Service, Trojan Special Purpose Integrated Remote Intelligence Terminal, Combat Service Support Very Small Aperture Terminal).
- Coordinates satellite access requests (SARs) and deconflict frequencies.
- Resolves, reports, and coordinates with other agencies to resolve radio frequency conflicts.
- Secures access into the division network and monitors accesses and activities internal to the network.

D-5. **The G-6 Plans Cell**. The plans cell is responsible for developing future plans and Annex K to the order, performing JTF and ASCC coordination, and service provisioning planning for the division. The G-6 plans cell performs the following functions:

- Prepares, maintains and updates command information management estimates, plans and orders to include the Information Management Plan.
- ICW the G-3, establishes procedures for employing relevant information and information systems to develop the common operational picture.
- Coordinates, plans, and directs the development of the common operational picture within the main command post.
- Coordinates with staff sections to ensure information quality criteria (accuracy, timeliness, usability, completeness, precision, reliability) are maintained.
- Coordinates local information network capabilities and services.
- Monitors and reports status of information network; coordinates future network connectivity.
- Coordinates future command, control, communications, and computer operations interface with joint, coalition forces to include host nation.
- Conducts electromagnetic spectrum operational planning.
- Develops and publishes Annex K to the division OPORD.
- Plans the transition of responsibility for the tactical network from the division to permanent theater signal assets (ITSB/ESB or commercial/contract).

D-6. **Signal System Support Section**. This section performs the following functions:

- Manages the local equipment and facilities that collect, process, store, display, and disseminate information including computers (hardware and software) and communications as well as policies and procedures for their use.
- Monitors, manages, and controls organic communications systems that interface with the GIG
- Performs TAC NETOPS functions (network management, IDM, IA).
- Manages a set of integrated applications, processes and services that provide the capability for producers and users to locate, retrieve, and send/receive information

D-7. **Signal System Support Teams.** These teams, which are part of the signal system support section, performs the following functions:

- Installs, operates, maintains, and defends server data (SIPRNET) and military Internet (NIPRNET) in support of division command post operations.
- Manages installation and operation of division main and TAC command post LANs, to include cable/wire installation and troubleshooting.
- Installs command post cable and wire; coordinates and supervises team members in the construction, installation, and recovery of cable and wire communications systems and auxiliary equipment within division command posts.
- Forms a portion of the division Information Service Support Office.
- Installs and operates the division's IT help desk; provides e-mail assistance and other help desk functions.
- Assists division units with network installation and troubleshooting as directed by the G-6.

D-8. **The G-6 Signal System Integration Oversight (SSIO) Section**. The SSIO section performs the following functions:

- Oversees network certification for division units.
- Coordinates and tracks command, control, communications, and computer modernization.
- Coordinates and tracks command, control, communications, and computer sustainment
- Oversees contractor support.
- Coordinates and tracks command, control, communications, and computer maintenance.
- Coordinates collective command, control, communications, and computer systems training.

- Training and readiness oversight for BCT JNN teams.
- Coordinates communication systems commercialization.
- Coordinates division command, control, communications, and computer readiness exercises.
- Training and readiness oversight for division headquarters and assigned unit JNN teams.
- Supervises data support teams.
- Oversees the installation of division command post wire and cable, to include cable system installation in fixed facilities, which would be probable employment mode as a JTF/JFLCC.

DIVISION G-6 ROLES AND RESPONSIBILITIES

D-9. The G-6 is the principal staff officer for all matters concerning communications and networks. The G-6 has the technical oversight responsibility over the division information networks to include training and readiness of the division signal company. The G-6 is responsible for providing planning guidance to the division signal company to execute the command, control, communications, and computer plan in support of the division commander's intent. In executing the commander's intent, the G-6 directs any technical changes to the network. To make physical moves to signal equipment, the G-6 recommends FRAGOs to direct such movement to the G-3. He is responsible for advising the division commander, staff, and subordinate commanders on command, control, communications, and computer operational matters (staff responsibilities, technical guidance, and training and readiness responsibility).

STAFF RESPONSIBILITIES

D-10. G-6 staff responsibilities include the following:

- Prepares, maintains, and updates command, control, communications, and computer operations estimates, plans, and orders. Such orders often will cause for CM changes across multiple brigades.
- Monitors and makes recommendations on all technical command, control, communications, and computer operations.
- Acts as the ARFOR G-6 when needed. (Equipment and personnel augmentation may be required to support this mission.)
- Advises the commander, staff, and subordinate commanders on command, control, communications, and computer operations and network priorities for battle command (for example, changing bandwidth allocation to support the division main effort—a brigade reinforced with additional intelligence, surveillance, and reconnaissance assets).
- Directs technical changes to all portions of the division network via the TSO process.
- Acts as the JTF J-6, if required. (Equipment and personnel augmentation will be required to support this mission and will be provided by the theater-level units such as the theater G-6, a SC(T), or a signal brigade or ASCC as necessary.)
  Develops, produces, changes/updates, and distributes signal operating instructions.
- Prepares/Publishes command, control, communications, and computer operation's SOPs for division command posts.
- Coordinates, plans, and manages the division's electromagnetic spectrum operational environment within its AOR.
- Plans and coordinates with higher and lower headquarters regarding information systems upgrade, replacement, elimination, and integration.
- ICW G-2, G-3, and the assistant chief of staff, information operations (G-7), coordinates, plans and directs all IA activities and command, control, communications, and computer operations vulnerability and risk assessments.
- ICW the staff, actively coordinates with a variety of external agencies to develop the information and communications plans, manages the information network, obtains required services, and supports mission requirements.

- Confirms and validates user information requirements in direct response to the tactical mission.
- Establishes command, control, communications, and computer policies and procedures for the use and management of information tools and resources.

TECHNICAL AUTHORITY RESPONSIBILITIES

D-11. The G-6 technical oversight responsibilities include the following:

- Provides signal units assigned or attached to the division with direction and guidance during preparation of network plans and diagrams establishing the information network (WAN), including business and intelligence WANs.
- Plans and integrates information systems and battle command equipment due to unit task organization/reorganization.
- ICW the ASCC and JTF, plans and directs all NETOPS activities within the division area of operations.
- Utilizes the NOSC as his eyes and ears to the network, leverages the tools provided by the NOSC to manage and reconfigure the network as warranted.

TRAINING AND READINESS RESPONSIBILITIES

D-12. Training and readiness responsibilities include the following:

- Ensures the development of required skills to all signal personnel within the division area of operations.
- ICW the assistant chief of staff, personnel (G-1), identifies requirements and manages the distribution of signal personnel within the division.
- ICW the G-3, monitors and provides oversight for information dissemination to adjust to changing warfighting function priorities and control measures within the division area of operations.
- Ensures automation systems and administration procedures for all automation hardware and software employed by the division are compliant with the GIG procedures and standards or Army specifications.
- Ensures, ICW the special troops battalion command, the division signal company is trained to support division missions and tasks during home station training events and deployments.

DIVISION NETOPS AND SECURITY CENTER

D-13. The division G-6 employs a fully integrated NOSC providing NETOPS functions for the division. All division signal elements must coordinate with the NOSC during the engineering, installation, operation, maintenance, management and defense of the division information network. The division NOSC has overall responsibility for establishing the division information network and provides the operational and technical support to all units assigned or attached to the division operating in the division area of operations.

D-14. The division NOSC performs the NETOPS activities, functions, and tasks required to create a dynamic and responsive network that quickly shifts priorities in order to support the ground tactical plan. This management function extends the strategic GIG's capabilities into the responsive, dynamic tactical formations. In order to increase responsiveness of a complex network and to facilitate the bandwidth required to support the division headquarters and brigade networks, the division employs a NETOPS cell with the regional network service center. The regional network service center flattens the TDMA satellite network structure and increases the bandwidth capability from approximately 6 Mbps to 40 Mbps, while the embedded NETOPS cell provides the management to enable the division network. The personnel composition of the NETOPS cell in supporting the network service center is mission, enemy, terrain and weather, troops and support available-time available and civilian driven.

D-15. In addition to expanding bandwidth, the division has the capability to dynamically reassign the bandwidth so that the communications support plan can match the division commander's ground tactical

plan. An example of this capability is the division designating a BCT as the main effort for an assault. As the main effort, the division commander gives the BCT a direct unmanned aerial surveillance sensor feed that must be broadcasted across the entire network. The division G-6 matches the communications support plan enabling the added, non-organic, capability by allocating a larger segment of the division enabled bandwidth.

D-16. The division NOSC provides an unprecedented capability that quickly provides capabilities to those who need it to enable the ground tactical plan. The division NOSC responsibilities include the following:

- ICW subordinate organizations, monitors, manages and ensures implementation of enterprise systems management/network management, IDM/CS, and IA/CND activities.
- Provides near real-time awareness of division networks and systems to the division G-6 and supporting service TNOSC/RCERT.
- Coordinates actions to resolve attacks/incidents on the division network with the service TNOSC and subordinate organizations.
- Coordinates operational procedures and requirements for IA/CND and information systems security with the supporting ASCC RCERT.
- ICW division signal company monitors, manages, and controls intra-division information network components.
- Monitors the operation of the networks in the division's subordinate units.
- Provides support and assistance to the subordinate NOSCs as required.
- Manages the organizational messaging system of record (Defense Message System, Tactical Message System) in the division, including managing network addresses and sub-domains.
- Coordinates operation and maintenance support of command, control, communications, and computer systems attached to support deployed division forces with the split-base and reach operations capability to the home base.
- Shares enterprise systems management/network management information with other management or monitoring centers.
- Provides the supporting service TNOSC with near real-time information on the status and performance of intra-division networks.
- Orders and accounts for all forms of COMSEC material, including storing keys in encrypted form and performing key generation and automatic key distribution.
- Performs COMSEC material accounting functions and communicates with other COMSEC elements.
- Performs IDM/CS functions to support all aspects of relevant information dissemination.
- Provides near real-time awareness of division networks and system that support the joint backbone to the JTF JNCC when the division is serving as the ARFOR.
- Informs the G-6 of network outages and shortcomings that require the electronic maintenance shop to rectify.

DIVISION SIGNAL COMPANY ORGANIZATION

D-17. The division signal company is subordinate to the division special troop's battalion and consists of the headquarters, G-6 and the signal detachment. In order to ensure the support of the division commander's intent, the division signal company installs, operates and maintains the network IAW technical guidance provided by the division G-6. The division G-6 technical oversight ensures the division network personnel and equipment are trained and maintained at the levels required to be successful. The organizational structure for the division signal company is depicted in Figure D-2.

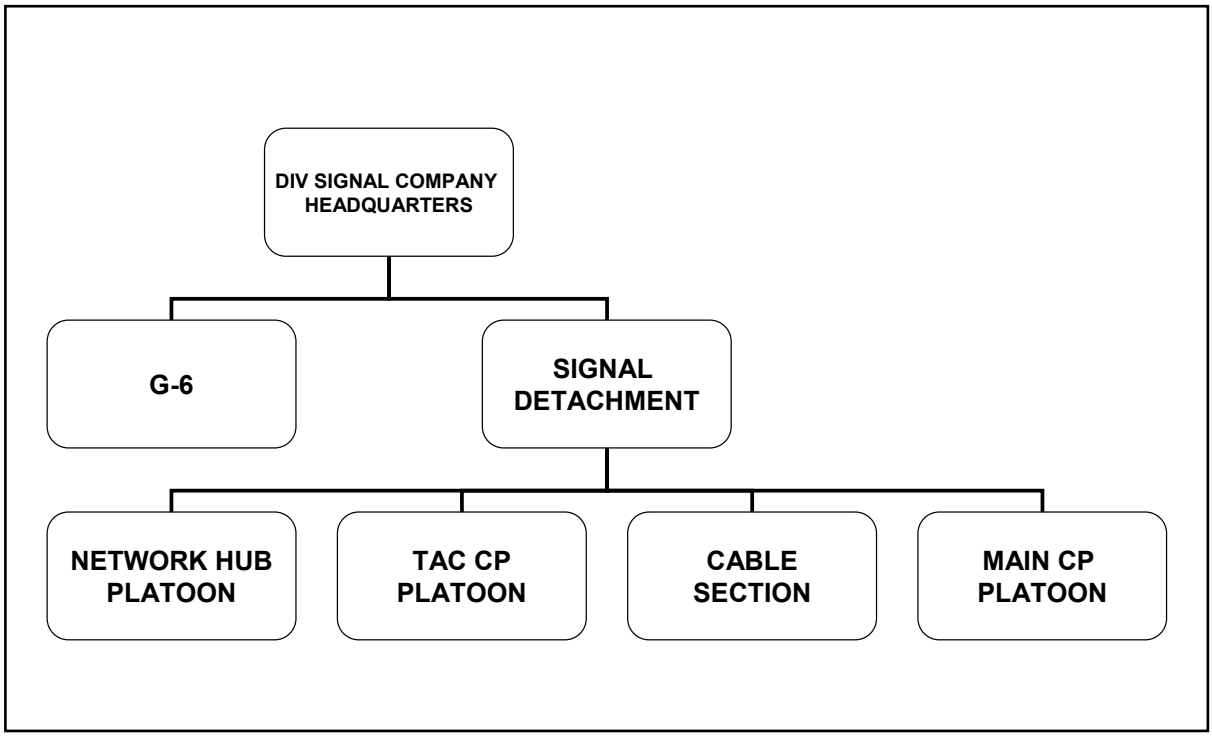

Figure D-2. Division signal company

HEADQUARTERS AND SIGNAL DETACHMENT

D-18. The headquarters provides logistics and maintenance support to the division signal company and consists of the company headquarters section. The signal detachment links the main command post with higher, adjacent, and subordinate headquarters and support activities. The signal detachment consists of the network hub platoon, the TAC command post platoon, a cable section and the main command post platoon. The elements of the headquarters and the detachment performs the following functions:

- **Company and detachment headquarters**. The company headquarters provides command and control to the company and is responsible for the administration and logistics support. The detachment headquarters provides the detachment command and control and limited NETOPS support.
- **Network hub platoon**. The detachment network hubs, provides TDMA and FDMA satellite connectivity. The network hub platoon consists of the TDMA and FDMA multiband section, the Baseband and Hub Support Sections. It installs, operates and maintains the network hub and satellite connectivity to the GIG.
- **Main command post platoon**. The main support platoon installs, operates and maintains the JNNs supporting the main command post.
- TAC command post platoon. The TAC command post platoon is designed to support the network services for the CP.
- **Cable Section.** The cable section provides the cable and wiring support for the command posts.

Appendix E

Brigade Combat Team and Battalion Network Management and Operations

The BCT performs NETOPS functions to maintain their WAN, LAN, common services, and information systems. Similar to the division, the BCT is required to operate its own network without augmentation from higher headquarters. This includes providing effective network management and IA across all organic networks. In addition, the BCT provides the organic common services of messaging, collaboration, storage, and security to its subordinate elements.

BRIGADE COMBAT TEAM MAIN COMMAND POST

E-1. The BCT main command post performs functions similar to the division main. This command post works future plans and participates with the BCT executive officer during the military decision making process. The BCT main writes the BCT Annex K and coordinates with higher, adjacent, and subordinate units during the orders development process.

BRIGADE COMBAT TEAM TACTICAL COMMAND POSTS

E-2. The BCT tactical command post is required to perform similar functions for the commander that the division tactical command post performed. These functions include the ability to produce FRAGOs and changes to current operations. The BCT tactical command post is also responsible for conducting all NETOPS associated with the current mission.

BATTALION NETWORK MANAGEMENT AND OPERATIONS

E-3. The battalion performs limited NETOPS functions and relies heavily on the support of the BCT S-6 for the reception of core common services, directory services, WAN accessibility, and IA. The S-6 staff performs all the planning and operations associated with the main and tactical command posts at higher headquarters. The S-6 holds the primary responsibility in developing the battalion Annex K input, LAN management, and connectivity coordination with the BCT and adjacent units. Figure E-1 displays battalions connected to the network.

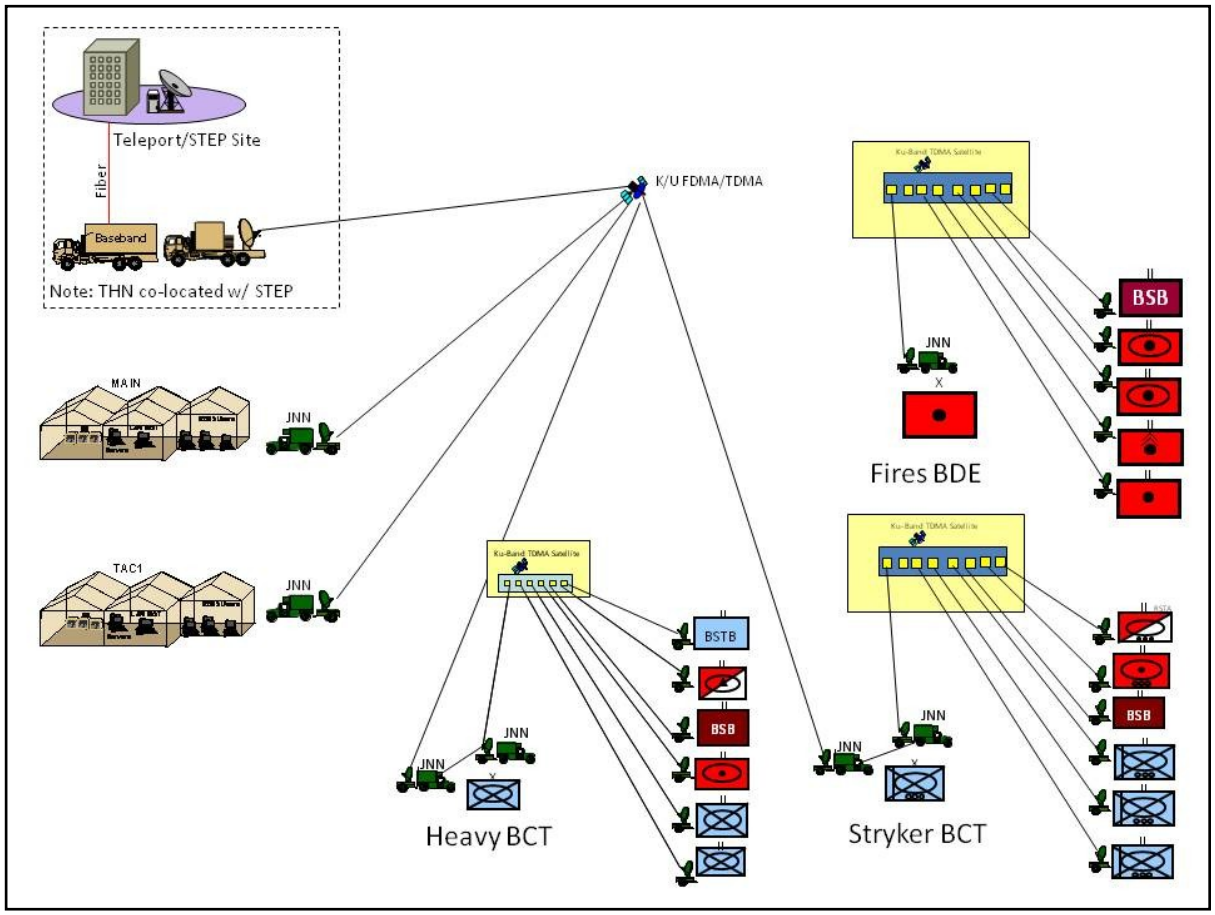

Figure E-1. Battalion Network Connections

Note. Appendix I outlines the procedures for JNN-N enabled/compatible units to request services from the FRHN.

Appendix F

LandWarNet Information Assurance Architecture Computer Network Defense View

This appendix presents the CND view of the LIAA. It is based on current best practices and existing technologies that can effectively counter the current threats to Army networks and systems. It also describes the overall goal for CND architecture for the Army, the components required to implement this architecture, as well as the policy that must be consistently applied across the architecture.

ARMY HIGH-LEVEL CND COMPUTER NETWORK DEFENSE DESIGN

F-1. As the networks of the Army proliferate and become more intertwined, it has become more difficult to define an external perimeter at which to place boundary CND components and thereby protect all systems and networks within. The recommended DID strategy then has become more of a distributed DID concept, which is composed of the items outlined in the paragraphs below and shown in Figure F-1.

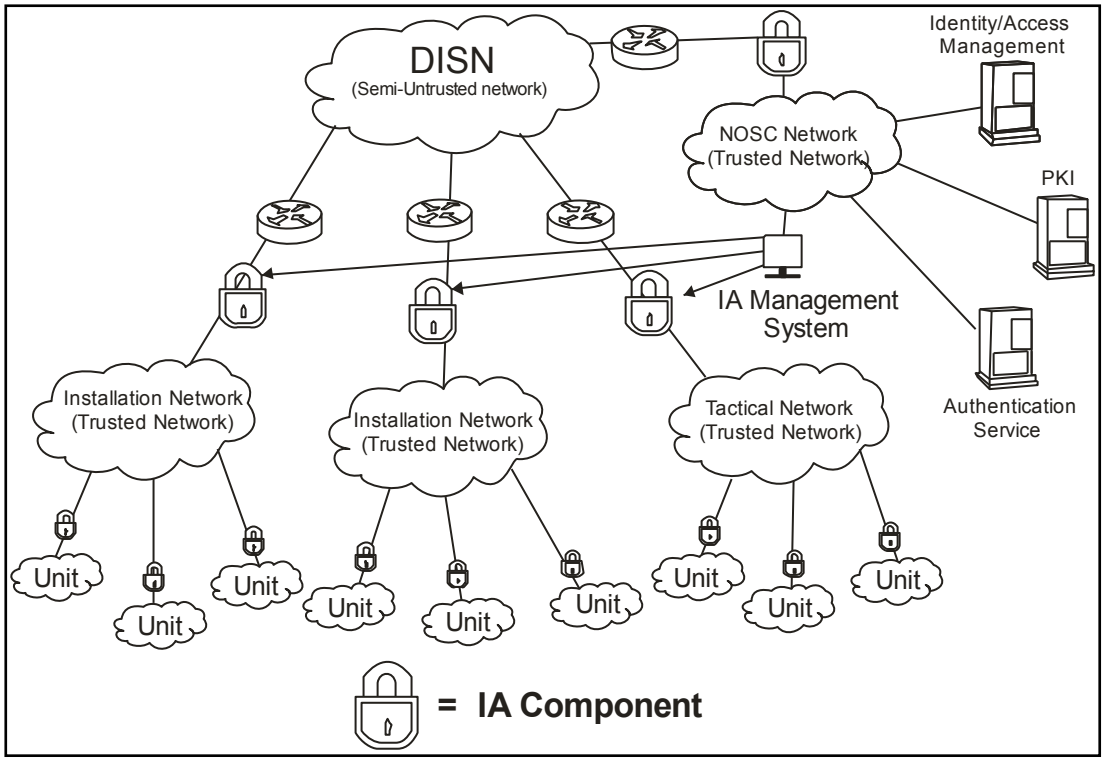

Figure F-1. Distributed defense in depth decentralized IA management/components

DISTRIBUTED DID

F-2. The Army CND perimeter will be a distributed, controlled, somewhat virtual perimeter. The Army distributed perimeter is defined as any gateway that connects to the DISN, JTF network, or the Internet. These networks will only be trusted to deliver packets. When packets arrive from these networks at the Army distributed perimeter, they will not be trusted. The LIAA will deploy perimeter protection at every connection to the DISN or the Internet. In general, connectivity to the Internet should be provided by the NIPRNET; however, it is understood that, on occasion, the Army does connect networks to the Internet.

F-3. In the strategic environment, DISN connections are typically implemented at the installation level, although in the future this may occur at GIG bandwidth expansion sites for many installations. In the tactical environment, DISN or JTF network connections are typically implemented at echelons above corps, corps, and division. However, with the fielding of the JNN for the 3ID, the ability to connect to the DISN will be provided at the unit level.

F-4. The LIAA CND view will provide an additional layer of protection at the enclave level. Enclaves are networks that are contiguous within installation and tactical networks. For example, a LAN connected to the installation network and operated by a tenant organization is considered an enclave. A command post LAN is another example of an enclave. These enclaves are under the authority of one commander/director who is responsible for protection within his AOR. The LIAA will deploy standard enclave protection at the gateways between the enclave network and its installation or tactical network.

F-5. The final layer of protection specified by the LIAA CND view is client and server systems' host protection. To the extent possible, enterprise-licensed security software and configuration standards will be used to provide this last layer of defense.

F-6. Management of the LIAA CND view will be centralized to the greatest extent possible. Centralized IA management of perimeter protection CND components will be performed by the TNOSCs within each theater. The TNOSCs will be resourced with the necessary tools and skilled personnel to configure, monitor, and manage these components. TNOSC personnel will also be trained in Army security policy related to perimeter protection to ensure that Army policy is implemented. The real-time demand of tactical signal units may require collocation of TNOSC personnel with tactical units to ensure that the commander's needs are met in terms of network connectivity and IA. Management of enclave and host protection CND will be the responsibility of the unit or organization that operates the enclave. Within strategic environments, it is expected that DOIM will perform this function with TNOSC guidance/oversight. Within tactical environments, unit signal personnel will perform this function.

F-7. The LIAA CND view specifies that certain IA components will be implemented such that they can provide services to the entire Army enterprise. For example, AD can provide enterprise-wide identification and authentication services for Windows platforms. The DOD PKI will be extended into Army tactical environments to provide the supporting infrastructure for public key enabled (PKE) applications. Enterprise access management products can provide single sign-on and common Web portal access services for applications across the Army enterprise. It is the intent of the LIAA CND view to maximize use of these enterprise-wide services to ensure consistency of implementation across the enterprise.

PERIMETER PROTECTION ARCHITECTURE

F-8. Figure F-1 illustrates the placement of perimeter protection at Army-DISN gateways. A standard architecture and suite of CND components will be used at every Army-DISN gateway. The primary objectives of the perimeter protection architecture are to:

- Stop intrusion attempts from entering Army networks; prevent malicious code from entering or leaving Army networks.
- Prevent use of frequently used outbound protocols such as the DNS, HTTP, and Simple Mail Transfer Protocol (SMTP) from being exploited by Trojan horse.
- Prevent the download of malicious mobile code through browsers.

- Prevent the use of objectionable Web sites for non-business purposes.
- Monitor packets entering or leaving Army networks to detect if any of these unauthorized activities are occurring.

F-9. To counter these threats, the LIAA CND view specifies the implementation of demilitarized zones at Army-DISN gateways. The demilitarized zone will host all publicly accessible systems for a particular installation or tactical network. This would include Web and e-mail servers primarily, but could also allow for the relocation of File Transfer Protocol (FTP) or other servers generally considered to expose a network to external threats. Limiting network traffic flow from anonymous users on the NIPRNET or Internet-to-Web, e-mail, or FTP servers on the demilitarized zone restricts the number of target systems potential attackers can attempt to exploit. Army administrators can then focus their host protection efforts on securely maintaining these few servers on the demilitarized zone.

F-10. Figure F-2 illustrates the architecture for a standard Army demilitarized zone. The CND components that will be implemented as part of the standard perimeter protection architecture are firewalls, gateway anti-virus scanners, screening Web proxies, and network intrusion detection system (NIDS) devices. The purpose of the gateway anti-virus scanner at the perimeter is to provide anti-virus detection for the most common traffic traversing the demilitarized zone: Web (HTTP, HTTP with Secure Sockets Layer [HTTPS]), e-mail, and FTP. Centralized management of the anti-virus scanner will improve the Army's ability to defend against new viruses by providing a central point where virus definition updates can be quickly applied.

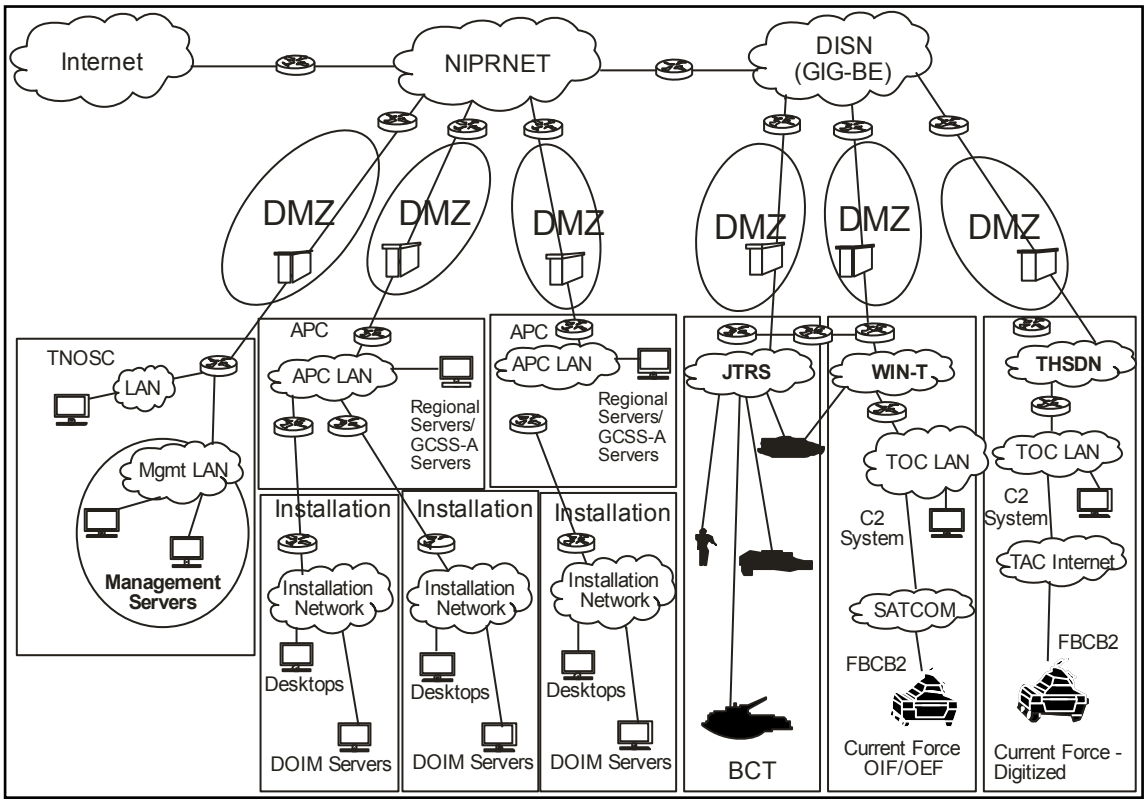

Figure F-2. Perimeter protection placement

F-11. The purpose of the screening Web proxy or Web security device is to examine outgoing Web traffic and ensure that it is valid HTTP or HTTPS traffic. These devices prevent the use of HTTP/HTTPS as a tunneling protocol for Trojan horses. In addition, these devices can maintain a list of objectionable Web sites and block user access to these sites, resulting in greater network bandwidth efficiency. Finally, the

Web security device can perform content filtering, which provides the ability to scan for sensitive keywords. This process can help ensure that sensitive information is not being exfiltrated from Army sites.

F-12. Firewalls, or in the future, IPSs, are used in the perimeter protection architecture to control network traffic flow based on a centrally controlled security policy. NIDS devices will also be deployed on the demilitarized zone. NIDS will provide the ability to detect intrusion activities that originate from the DISN or Internet. By placing the NIDS on the demilitarized zone segment, the number of alerts generated by the NIDS should be significantly reduced because the firewall will be blocking most network protocols. (See Figure F-3.)

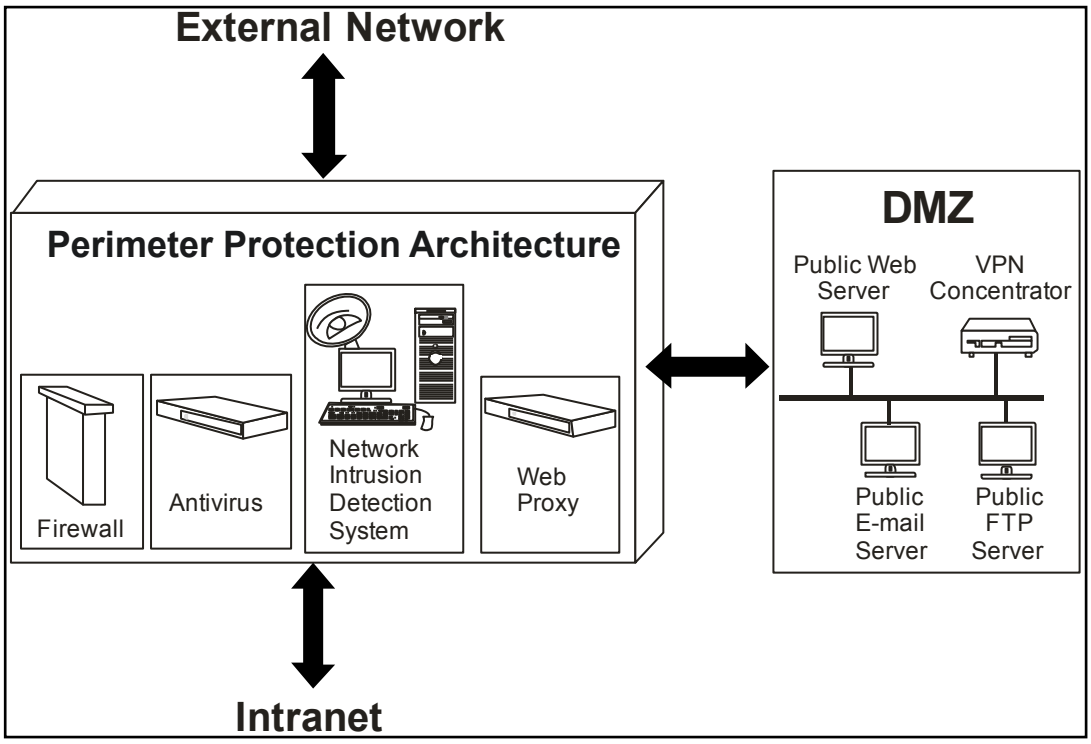

Figure F-3. Perimeter protection architecture

F-13. In addition to external access to the public demilitarized zone, the perimeter protection architecture will support the implementation of Army extranets. Extranets are site-to-site connections that will use the DISN or Internet as the communications backbone for the connection. Figure F-4 illustrates two examples of Army extranet connections. The first example shows a desktop Global Combat Support System-Army client system on one installation network accessing a Global Combat Support System-Army server on another installation's network. In this case, the NIPRNET is used to provide the connection between the two installations. The perimeter protection at the client system's installation will enforce a policy that allows the client system to access only the Global Combat Support System-Army server within the other installation's network. The perimeter protection at the server's installation will allow only that client system to access the server.

F-14. In the second example, a current force unit and a digitized unit are operating within an area of operations. In this case, the SIPRNET is used to provide the connection between the two units. The perimeter protection at the digitized unit gateway will enforce a policy that allows a command and control system on the current force network to access only the command and control system within the digitized unit's network. The perimeter protection at the current force gateway will allow only the command and control system on the digitized unit network to access its command and control system.

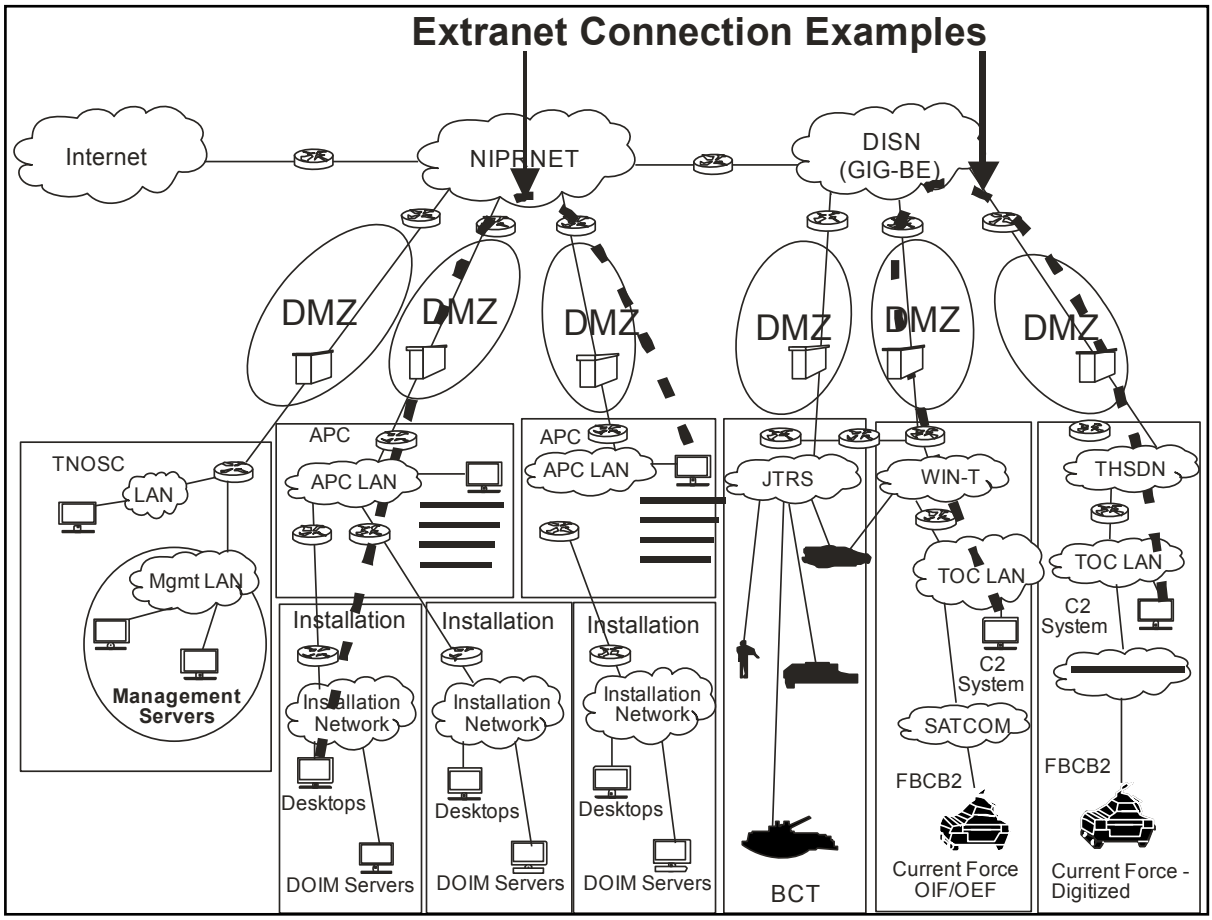

Figure F-4. Extranet connection example

F-15. Access for extranet connections will be permitted or denied by perimeter protection firewalls. In some cases, the additional protection of encrypted communications between Army sites may be desired by a commander or director. The perimeter protection architecture will be capable of providing site-to-site VPN encryption. These site-to-site VPN connections can be implemented using Internet Protocol Security that is performed by the firewall. The VPN end points will be the respective sites' firewalls to allow the NIDS devices at those sites to monitor network traffic coming from the extranet connection.

PERIMETER PROTECTION ARCHITECTURE

F-16. The following sections discuss the implementation of public access policy and extranet policy within the perimeter protection architecture.

Public Access Policy

F-17. The public access policy refers to the firewall access control policies that apply to perimeter protection demilitarized zones. These policies will be applied enterprise wide at all Army sites. These policies will be controlled by the CIO/G-6 and will require CIO approval to modify. This central control is necessary because public access presents the greatest risk to the Army enterprise. Public access in this case is defined as any anonymous packet that originates from the DISN or Internet and is allowed to enter the demilitarized zone. For example, contractors accessing AKO, family members accessing unit Web sites, mobile users accessing VPN concentrators, and e-mails from friends, families, and business partners are

examples of connections from anonymous hosts that require access to Army networks and resources. Figure F-5 illustrates the public access policy overlaid onto the perimeter protection architecture.

F-18. The Public Access Policy specifies that the following protocols will be permitted from anonymous DISN and Internet IP addresses to the demilitarized zone servers (Unless specifically mentioned, all other protocols will be denied access by the firewall)—

- HTTP will be permitted from anonymous IP addresses to public Web servers on the demilitarized zone.
- HTTPS will be permitted from anonymous IP addresses to public Web servers on the demilitarized zone.
- SMTP will be permitted from anonymous IP addresses to public e-mail servers on the demilitarized zone. This type of network traffic will be routed through the gateway's anti-virus device before it is sent to public e-mail servers.
- If external FTP services are required, then FTP is permitted from anonymous IP addresses to public FTP servers on the demilitarized zone.
- If remote users require VPN access to a VPN concentrator, then Internet Protocol Security (IP protocol 50), Internet Key Exchange (User Datagram Protocol port 500 and 4500), and Authentication Header (IP protocol 51) are permitted from anonymous IP addresses to VPN concentrators on the demilitarized zone.
- No protocols will be permitted from demilitarized zone servers to the external network.

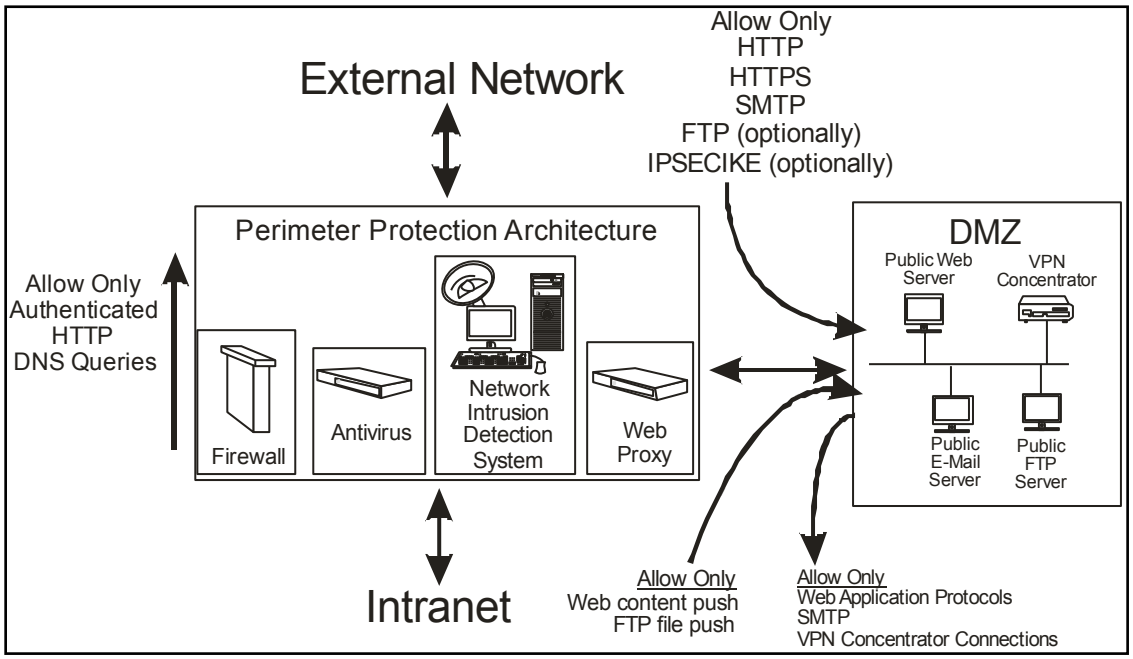

Figure F-5. Perimeter protection—public access policy

F-19. The Public Access Policy specifies that the following protocols will be permitted from demilitarized zone servers to servers within the internal network (Unless specifically mentioned, all other protocols from the demilitarized zone to the internal network will be denied by the firewall)—

- If the public Web server on the demilitarized zone hosts active content, the Web server may connect to application servers on the internal network using the minimum required protocols to implement the connection. Examples of these protocols may be Netscape Application Programming Interfaces, Java 2 Platform Enterprise Edition, and .NET protocols.
- SMTP will be permitted from the e-mail server on the demilitarized zone to e-mail servers on the internal network.

- If a remote access VPN concentrator resides on the demilitarized zone, then a limited set of protocols will be permitted from the VPN concentrator to the internal network. These protocols include Post Office Protocol and Internet Message Access Protocol for e-mail; HTTP and HTTPS for Web; Telnet and FTP for system administrators; Lightweight Directory Access Protocol for Windows AD login; and Network Basic Input/Output System protocols for Windows Networking.

F-20. The Public Access Policy specifies that the following protocols will be permitted from servers within the internal network to demilitarized zone servers (Unless specifically mentioned, all other protocols from the internal network to the demilitarized zone will be denied by the firewall)—

- The Secure Shell Protocol will be used to push Web content to the public Web server. Secure Shell will be permitted from the internal network to the public Web server on the demilitarized zone.
- The Secure Shell Protocol will be used to push files to the public FTP server. Secure Shell will be permitted from the internal network to the public FTP server on the demilitarized zone.

F-21. The Public Access Policy specifies that the following protocols will be permitted from the internal network to the external network (Unless specifically mentioned, all other protocols from the internal network to the external network will be denied by the firewall)—

- DNS will be permitted from internal DNS servers to DISN or Internet Service Provider DNS servers. This will allow name resolution of external IP addresses.
- HTTP and HTTPS will be permitted from internal network IP addresses to the external network. These protocols will be routed through the Web proxy to provide Web security.

Extranet Access Policy

F-22. Extranet Access Policy refers to the firewall access control policies that apply to Army site extranet connections. These policies will be implemented by the TNOSCs but specified by the local site's commander or director. TNOSC personnel will provide advice to commanders/directors to help them decide which protocols present an acceptable level of risk. The policies specified herein provide guidelines for TNOSC personnel on implementing the Extranet Access Policy. Figure F-6 illustrates the Extranet Access Policy overlaid onto the perimeter protection architecture.

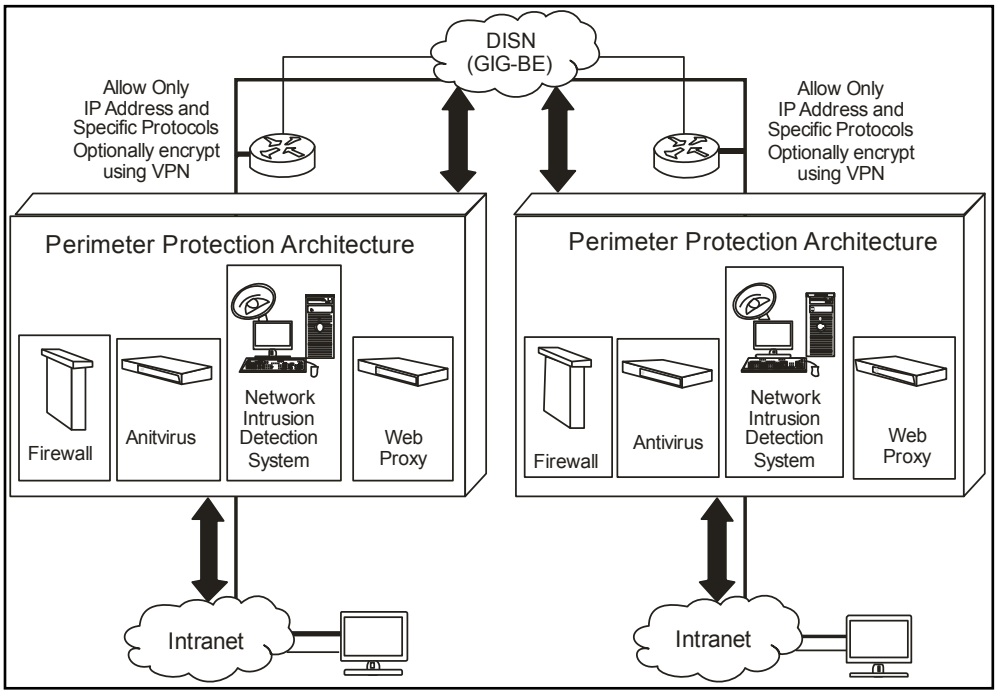

Figure F-6. Perimeter protection—extranet access policy

F-23. The following is a summary of the Extranet Access Policy:

- Extranet connection rules should limit the number of permitted source IP addresses to the minimum number of hosts required to implement the extranet connection. Rules that allow entire subnets to access an extranet connection are discouraged.
- Extranet connection rules should limit the number of permitted destination IP addresses to the minimum number of hosts required to implement the extranet connection. Rules that allow source IP addresses to access entire subnets are discouraged.
- Extranet connection rules should limit the number of permitted protocols to the minimum required to implement the extranet connection.
- The use of remote execution protocols should be discouraged. Remote execution protocols are protocols that allow users to execute commands on a remote system. Potential attackers can use these protocols to leapfrog from system to system and site to site.
- The use of certain Internet Control Message Protocols over extranet connections such as echo-request and echo-reply should be discouraged to prevent denial-of-service attacks.
- SMTP or Microsoft Exchange should not be permitted through an extranet connection. Mail server connections should be performed through the public e-mail server so that the gateway anti-virus device can scan incoming and outgoing e-mail messages. Allowing e-mail exchanges through the extranet connection will bypass the anti-virus scanner and could facilitate the spread of malicious code carried by e-mail.

ENCLAVE PROTECTION ARCHITECTURE

F-24. Figure F-7 illustrates the placement of enclave protection at command post LANs and installation enclaves. A standard architecture and suite of CND components will be used at every gateway between command post LANs and Army tactical networks or tenant organization LANs and installation networks. The primary objectives of the enclave protection architecture are to stop insider intrusion attempts, prevent the spread of malicious code through Army networks, prevent denial-of-service attacks that originate from within Army networks, and monitor packets entering or leaving enclaves to detect if any of these unauthorized activities are occurring.

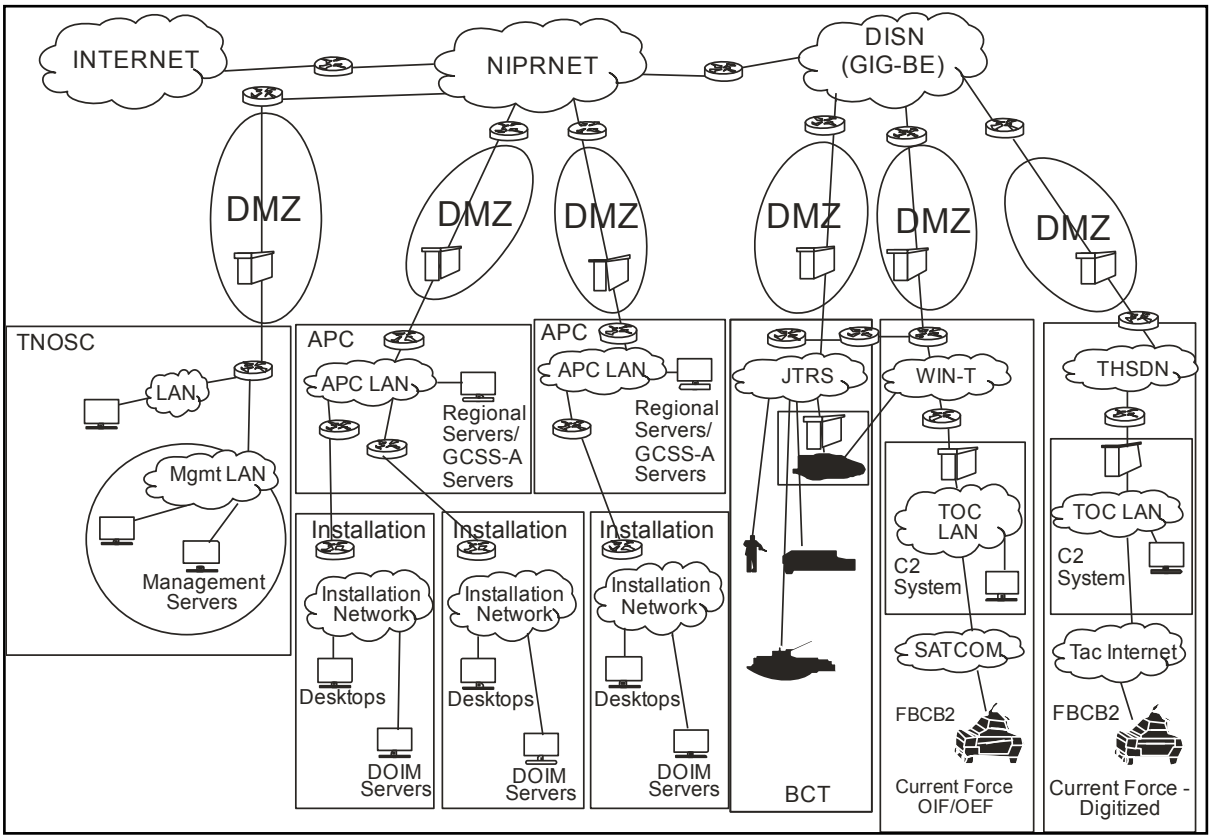

Figure F-7. Enclave protection placement

F-25. Figure F-8 illustrates the CND components used in the enclave protection architecture. The architecture consists of firewalls, or in the future, IPSs and NIDSs. The firewalls are used in the enclave protection architecture to control network traffic flow based on a locally controlled security policy. NIDS devices will provide the ability to detect intrusion activities, worms, and Trojan horses that originate from within Army networks. By placing the NIDS on the enclave LAN interface of the firewall, the number of alerts generated by the NIDS should be significantly reduced because the firewall will be blocking most network protocols. The use of NIDS in some tactical circumstances is optional. For small deployments where unit-trained personnel are not available to operate the NIDS, the unit may decide to forego use of NIDS on command post LANs. However, a NIDS must always be used as part of the perimeter protection architecture. For installations, it is expected that enclave protection will be managed by the TNOSCs with input on policy from local commanders/directors and their staff.

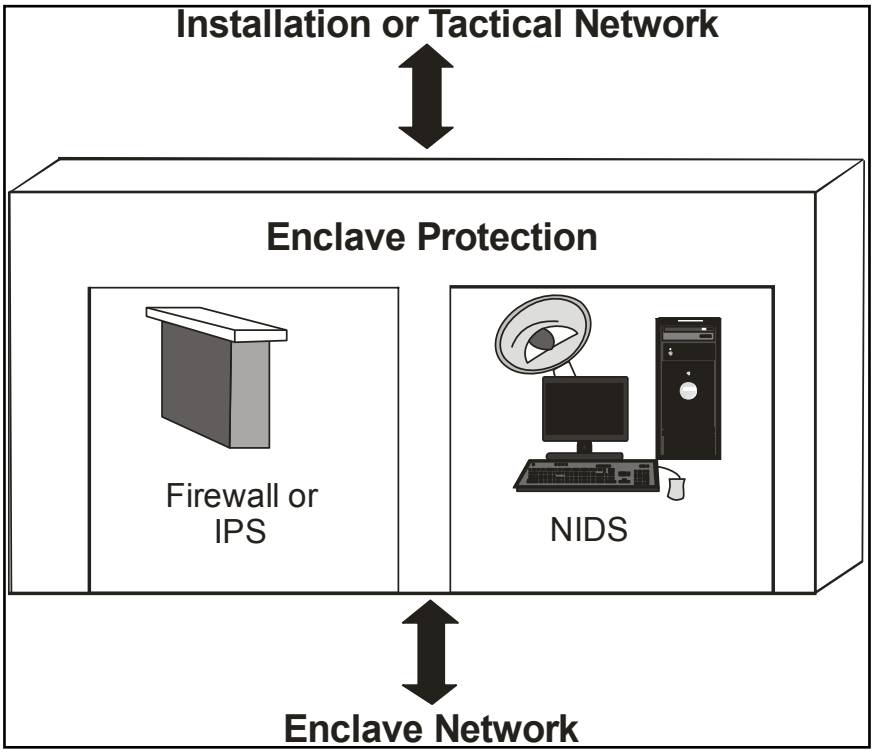

Figure F-8. Enclave protection architecture

Enclave Access Policy

F-26. Enclave Access Policy refers to the firewall access control policies that apply to Army enclave-to-enclave connections. These policies will be implemented by the TNOSCs but specified by the local site's commander or director. TNOSC personnel will provide advice to commanders/directors to help them decide which protocols present an acceptable level of risk. The policies specified herein provide guidelines for TNOSC personnel on implementing Enclave Access Policy. Figure F-9 illustrates the Enclave Access Policy overlaid onto the enclave protection architecture.

F-27. The following is a summary of the enclave protection policy:

- Enclave connection rules should limit the number of permitted source and destination IP addresses to the minimum number of hosts required to implement the enclave-to-enclave connection.
- Enclave connection rules should limit the number of permitted protocols to the minimum required to implement the enclave-to-enclave connection.
- The use of remote execution protocols should be discouraged. Potential attackers can use these protocols to leapfrog from enclave to enclave.
- The use of certain Internet Control Message Protocols over extranet connections such as echo-request and echo-reply should be discouraged to prevent denial-of-service attacks.

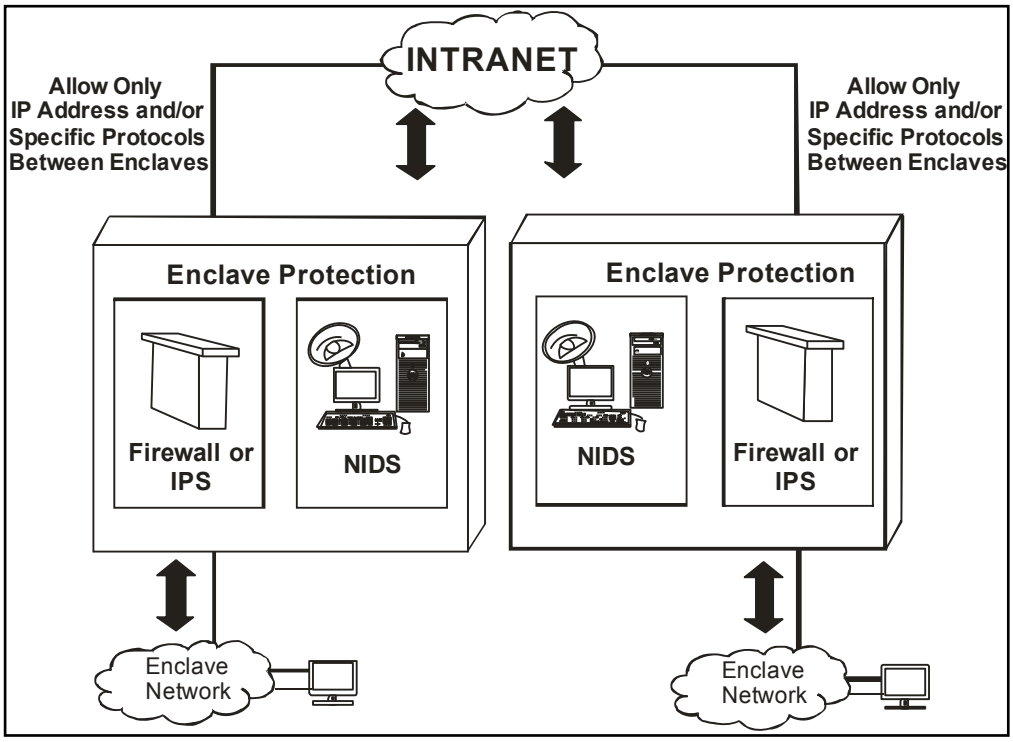

Figure F-9. Enclave protection policy

HOST PROTECTION

F-28. The final protection level in the LIAA CND view is the host protection level. It is the goal of the US Army to employ host-based IDS software, anti-virus software, personal firewall software, and patch management agents on all workstations and servers. In addition, critical servers should implement file integrity tools as well. The Army has enterprise licenses for both personal firewalls and anti-virus software through the DOD. Because of the availability of these enterprise licenses, the Army can deploy these applications on every system. However, with host-based IDS devices, file integrity tools, and patch management software, there may not be the same latitude. It would be optimal for the Army to acquire enterprise licenses for these applications, but if that is not financially feasible, choices must be made regarding which systems will be configured with host-based IDS software and patch management agents. It may be necessary to initially configure only critical servers, such as demilitarized zone servers and data center servers, with this software if there is a limited license. In addition to host protection software, Army host system protection will be accomplished by:

- Implementing relevant security patches as defined by IAVAs.
- Secure configuration of operating systems using DOD and Army Security Technical Implementation Guides (STIGs) http://iase.disa.mil/stigs/stig/index.html
- Secure configuration of database management systems using DOD and Army STIGs.
- Secure configuration of standard applications, such as Web servers, using DOD and Army STIGs.
- Strong password/authentication for Windows networking using AD.
- Use of enterprise IA services, such as Common Access Card, PKI, and PKE applications.

F-29. While most users will access resources locally using Smartcard-based Logon, mobile and home users may use non-Army systems to remotely access e-mail and other enterprise services. Because these systems may not be configured to Army standards, the access granted to these systems will be limited. It is expected

that these users will access Army enterprise services through remote access VPNs. In the future, the Army may consider using emerging commercial products that check host systems for patches, personal firewall activation, and anti-virus update status prior to allowing a connection to the network.

CENTRALIZED IA SERVICES

F-30. The LIAA CND view specifies that certain IA services will be implemented so they can provide services to the entire Army enterprise. This will ensure consistency of implementation across the enterprise while reducing the overall cost of implementing these services. In reality, some of the services may be provided at the DOD level by DISAs Net-Centric Enterprise Services program. It is anticipated that the following core services are to be implemented in Net-Centric Enterprise Services Increment 1:

- Single sign-on.
- Role-based access control.
- Data/eXtensible Markup Language/Simple Object Access Protocol classification labeling.

F-31. The enterprise IA services provided by the Army are intended to be in addition to Net-Centric Enterprise Services, and will only be developed in response to unique Army IA requirements. The following services are needed to fulfill Army unique needs:

- **PKI**. The DOD PKI provides the necessary infrastructure to support PKE applications. This includes key generation facilities, directory services, Common Access Card tokens, registration authorities, compromise recovery capabilities, and key recovery capabilities. This infrastructure primarily exists in strategic environments. The Army is just beginning to examine extending PKI support into the tactical environment.
- **AD**. The Army is migrating to AD in order to provide a number of centralized services for Windows systems. With the migration to AD, the following security-relevant services will be available to Army systems: strong Kerberos-based authentication, group policy management that can be used to implement STIGs and patches, and some secure directory services. AD is more prevalent in the strategic environment, but the Army is actively pursuing implementation in the tactical environment.
- **Single sign-on**. Currently, AKO provides single sign-on authentication for multiple applications. It is envisioned that this service could be extended to other Web portals that are hosted on Army public Web servers. Additional activity should be focused on consolidating Army Web applications into portals that provide users access to multiple applications through a single login. This will enhance the Army's ability to centrally manage IA at these portals with the added benefit of relieving users of the need to login to multiple applications.

CENTRALIZED IA MANAGEMENT

F-32. The key to the concept of CND is real-time IA management. This includes the ability to configure CND components, monitor IA sensors, and provide the analysis necessary to properly react in the event of an attack. The benefits of a centralized approach are that it ensures consistency of IA implementation across the enterprise IAW Army IA standards and minimizes the number of personnel with the highly specialized skills needed to perform IA. Table F-1 summarizes the roles and responsibilities related to IA management of specific LIAA CND protection levels.

Table F-1. IA management responsibilities of LIAA CND protection levels

Protection level	*Responsible organization*
Perimeter Protection—Public Access	CIO/G-6 determines public access policy. TNOSC manages perimeter protection CND components within a theater.
Perimeter Protection—Extranet Access	Local commander/director for installation or tactical unit determines extranet access policy, with guidance from TNOSC IA personnel. TNOSC manages perimeter protection CND components within a theater.
Enclave Protection	Local commander/director for enclave determines enclave access policy, with guidance from TNOSC IA personnel. TNOSC manages enclave protection CND components within a theater. At the discretion of the commander, signal personnel within a unit may take over this responsibility.
Host Protection	Local commander/director for enclave has overall responsibility for host protection implementation and compliance. At installations, DOIM will manage host protection.
Centralized IA Services	Net-Centric Enterprise Services, which will include the DOD PKI, is managed by DISA. AKO and AD is managed by NETCOM.

F-33. The following IA management functions will be performed by the TNOSCs/RCERTs:

- **IA event monitoring and correlation**. While commanders and installations will still have the ability to view IA activity, they will not be responsible for providing IA event monitoring and event correlation. The TNOSC will collect data from perimeter protection and enclave protection CND components. Due to the size and complexity of the LWN, the TNOSC will employ security information management tools to provide event monitoring, event correlation, and data reduction support for analysts.
- **Incident response**. When an IA event is detected, the TNOSC will work with the collocated RCERT to resolve IA incidents. Events of interest identified by analysts performing IA event monitoring will be investigated from the RCERT ICW the TNOSC. If the response involves a centrally managed CND component, the TNOSC will coordinate with CIO/G-6, unit commanders, installation commanders/directors, and enclave commanders/directors and take actions to counter the attack. These actions may include changing firewall policies, applying patches, restricting Web access, or removing systems from the network. If the response involves a locally managed LAN, the TNOSC will work with local administrators. The RCERT will also coordinate with the ACERT to publish significant information to interested parties.
- **VPN management**. TNOSCs will manage VPN hardware and software. This includes extranet VPNs and remote access VPNs. Under certain circumstances, tactical VPNs between enclaves may require local management (i.e., where connectivity to a TNOSC is not possible). However,

under normal conditions, the TNOSC service desk will manage the provisioning of VPN services between various installations, between the APCs, and between installations and the APCs.

- **IA system/Device management**. All CND components (i.e., firewalls, IPS, NIDS, gateway anti-virus, and gateway Web security devices) will be managed from the TNOSC. Management includes CND components at the perimeter and enclaves. Management functions include CM of firewall policies, CM of CND component software, pushing updates of anti-virus definition files to gateway anti-virus devices, pushing updates of attack signatures to NIDS devices, pushing updates of objectionable Web sites to Web security devices, and maintaining CND component hardware.
- **Formal communications**. As the Army transitions to a centralized IA management construct, a formal communications process will be implemented between commanders and the TNOSC. The individual commanders must have a way to communicate information regarding their networks to the individuals now tasked with monitoring and managing the IA devices on those networks. This includes strategic as well as tactical environments. Without this type of interaction, the TNOSC will be working in a void, with limited information regarding the network they are trying to protect. The input by commanders to the TNOSC/RCERT will provide significant and critical information about the environment being monitored, allowing for more accurate determination of security events.
- **Secure configurations guidance**. STIGs are provided to the A-GNOSC by DISA for use on Army systems. The configurations then become part of the Army Golden Master Program. The A-GNOSC uses the distribution network of the TNOSC to provide this information. All STIGS are published from the TNOSC, although actual hands-on configuration is performed by local administrators. Configurations are allocated through the Systems Management Function, as needed, to installations and tactical units. Some tactical systems are exempt from this configuration control.
- **Vulnerability assessments**. As part of the system life cycle, vulnerability assessments will be performed on workstations and servers to ensure that they remain secure. Computer Defense Assessment Program assistance can be requested from the servicing RCERT.

F-34. The tools required by the TNOSC to perform these functions are firewall enterprise management systems, security information management systems, security compliance management software, network vulnerability scanners, asset inventory software, and network discovery software. Only those IA tools approved by National Security Agency/DISA will be used.

F-35. The following IA management functions will be directed by commanders and directors and implemented by the DOIM in strategic environments and signal personnel in tactical environments. The tools required by DOIM and signal personnel to perform these functions are firewall enterprise management systems, security compliance management software, network vulnerability scanners, and network discovery software. IA management function include:

- **Formal communications**. As mentioned above, IA device management will be the responsibility of the TNOSC. For extranet and enclave access policies, commanders and directors will need to communicate with TNOSC personnel to develop these policies. A formal communications methodology will be developed to facilitate this communication. In some cases, the communications mechanism may consist of collocating TNOSC personnel with the unit during tactical deployment or to installations.
- **IA system/device management**. Host protection software will be managed locally. The local commander or director will ensure that software is loaded and configurations are managed and updated as defined by Army standards or IAVAs.
- **Secure configurations guidance**. The local commander or director at strategic sites will ensure that hosts under their purview are configured IAW Army-published STIGs. For tactical systems, the acquisition organization (e.g., PEO, program manager) responsible for acquiring the system will ensure that hosts under their purview are patched IAW Army published STIGs.

- **Patch management**. The local commander or director at strategic sites will ensure that hosts under their purview are patched IAW published IAVAs. For tactical systems, the acquisition organization responsible for acquiring the system will ensure that hosts under their purview are patched IAW published IAVAs.
- **Vulnerability assessments**. As part of a proactive IA program, the local commander or director may authorize vulnerability assessments on workstations and servers to ensure that they are in compliance with IAVAs and STIGs. The local commander or director should coordinate with TNOSC personnel so that vulnerability assessment activities are not treated as intrusion events.

IA/CND TRAINING REQUIREMENTS

F-36. The following paragraphs discuss IA/CND training requirements.

USER TRAINING

F-37. To support the Soldier in a highly effective and professional manner, the Army must ensure that appropriate levels of IA awareness, training, education, certification, and workforce management are provided to the IA workforce and information system users that commensurate with their respective responsibilities.

F-38. Users are the foundation of the DID strategy, and their actions affect the most vulnerable portion of the AEI. Users must hold a security clearance or access approvals commensurate with the level of information processed or available on the system. All users must receive an Initial Security Awareness Briefing training tailored to the system and information accessible before issuance of a password for network access. Users must have training in security awareness annually thereafter. The Initial Security Awareness Briefing will include the following:

- Threats, vulnerabilities, and risks associated with the system. This portion will include specific information regarding measures to reduce malicious logic threats; principles of shared risk, external and internal threat concerns; acceptable use privacy issues prohibitions on loading unauthorized software or hardware devices; and the requirement for frequent backups.
- Information security objectives (that is, what needs to be protected).
- Responsibilities and accountability associated with IA.
- Information accessibility, handling, and storage considerations.
- Physical and environmental considerations necessary to protect the system.
- System data and access controls.
- Emergency and disaster plans.
- Authorized system configuration and associated CM requirements.
- Incident, intrusion, malicious logic, virus, abnormal program, or system response reporting requirements.
- INFOCON requirements and definitions.

IAM TRAINING

F-39. IAMs are appointed at all appropriate levels of command. This includes major subordinate commands and generating and deploying forces (usually the division G-6). The IAM has overall responsibility for the unit's IA program to include project development, deployment, and management of unit software, operating systems, and networks. The IAM must be IA trained and certified, and must maintain his certification. All IAMs will hold a US government security clearance and access approval commensurate with the level of information processed by the system. A contractor will not fill the IAM position. Units will designate the IAM position IT-I, IT-II, or IT-III. Table F-2 provides the minimum IAM training requirements.

Table F-2. IAM training requirements

Step	*IAM training requirements*
1	Complete Initial Security Awareness Briefing.
2	Be appointed, on orders, as unit IAM.
3	Complete one of the following within 6 months of appointment: • The four day Army IAM course. • The e-Learning (SmartForce) modules in Information System. • The e-Learning (SmartForce) modules in Internet Security. • Other Service or commercial vendor courses.
4	Complete/Attend one of the following every 18-24 months: • A four-day Army IA workshop or a DOD-sponsored IA workshop. • The e-Learning (SmartForce) modules Securing Networked Information I or Securing Networked Information II. • The e-Learning (SmartForce) modules Microsoft or Unix. • Other Service or DOD IA workshops.
5	Annotate all training and training refresher in the Compliance Reporting Database Second Edition (A&VTR) within two weeks of course completion.

IANM/INFORMATION ASSURANCE NETWORK OPERATOR TRAINING

F-40. The commander of the unit responsible for the network appoints the IANM. The IANM is normally under the OPCON of the S-3. Units will appoint information assurance network operators (IANOs), as required, to assist the IANM. Units will designate IANM and IANO positions IT-I or IT-II. Each IANM and IANO must be IA and Vulnerability Assessment Technician certified. Table F-3 describes the minimum training requirements necessary to be appointed to an IANM or IANO position.

Table F-3. IANM/IANO training requirements

Step	*IANM/IANO training requirements*
1	Complete Initial Security Awareness Briefing.
2	Be appointed, on orders, as unit IANM or IANO.
3	Complete one of the following within 6 months of appointment: • The four-day Army IAM Course. • The e-Learning (SmartForce) modules in Information System Security. • The e-Learning (SmartForce) modules in Internet Security. • Other Service or commercial vendor courses.
4	Complete the 2 week Systems Administrator/Network Manager course within 6 months of appointment.
5	Complete/Attend one of the following every 18–24 months: • A four day Army IA workshop or a DOD sponsored IA workshop. • The e-Learning (SmartForce) modules Securing Networked Information I or Securing Networked Information II. • The e-Learning (SmartForce) modules Microsoft or UNIX. • Other Service or DOD IA workshops.
6	Annotate all training/training refresher in A&VTR within two weeks of course completion.

IASO TRAINING

F-41. The commander of the activity responsible will appoint an IASO (normally the unit's signal officer) for each information system or group of information systems that connect to the network. The G-6/S-6 has overall responsibility for the secure operation of the network and information systems at BCT and subordinate units. This function is performed by the DOIM or DOIMs representative in the generating and deploying forces. At the BCT, the G-6/S-6 normally assumes the role and responsibilities of the IASO. Table F-4 outlines the IASO training requirements.

SYSTEM ADMINISTRATOR/NETWORK MANAGER TRAINING

F-42. System administrators and network managers must be designated as IT-I, IT-II, or IT-III. Each system administrator/network manager must be trained, experienced, and currently certified on the information system they are required to maintain. The system administrator/network manager should be a US citizen. He must hold a US government security clearance and local access approvals commensurate with the level of information processed on the system or network. Table F-5 lists the system administrator/network manager training requirements.

Table F-4. IASO training requirements

Step	*IASO training requirements*
1	Complete Initial Security Awareness Briefing.
2	Be appointed, on orders, as unit IASO.
3	Complete one of the following within 6 months of appointment: • IASO Course. • DISA's Operational Information System Security compact disk-read only memory (CD-ROM). • The e-Learning (SmartForce) modules in both Internet Security and Net Safety. • Other Service or commercial vendor courses.
4	Complete/Attend one of the following every 18-24 months: • A four day Army IA workshop or a DOD sponsored IA workshops. • The e-Learning (SmartForce) modules Securing Networked Information I or Securing Networked Information II • The e-Learning (SmartForce) modules Microsoft or UNIX. • Other Service or DOD IA workshops.
5	Annotate all training/training refresher in the A&VTR within two weeks of course completion.

INFORMATION ASSURANCE VULNERABILITY MANAGEMENT

F-43. IAVM is the DOD program to identify and resolve discovered vulnerabilities in Army systems and platforms. It requires the completion of four distinct phases to ensure compliance. These phases are (1) vulnerability identification, dissemination, and acknowledgement; (2) application of measures to affected systems to make them compliant; (3) compliance reporting; and (4) compliance verification. This program includes IAVAs, IAVBs, and technical advisories.

F-44. A patch is an immediate solution provided to users once a bug is discovered and can often be downloaded from the software maker's Web site. Previously, patches required a manual touch at each device on the network coupled with the length of time an automated tool was required. An enterprise solution has been selected by DOD which is eEye Retina for scanning and Citadel Hercules for remediation.

F-45. Complete asset inventories (100 percent) will be conducted and reported to the A&VTR semi-annually as a minimum and after every IAVA. Every system administrator/network manager will register in

the A&VTR and record training as well as the assets for which they are responsible. Dissemination of IA technical tips, IAVBs, and IAVAs will automatically be forwarded upon registration completion. Interoperability testing will be performed prior to the application of system patches and fixes for interoperability compliance.

F-46. All IAVAs will be applied immediately. If the IAVA cannot be implemented, a mitigation plan must be submitted in A&VTR for approval/disapproval.

Table F-5. System administrator/Network manager training requirements

Step	*System administrator/Network manager training requirements*
1	Complete Initial Security Awareness Briefing.
2	Be appointed, on orders, as unit SA or network management.
3	Complete one of the following within 6 months of appointment: • The four-day Army IAM Course. • The e-Learning (SmartForce) modules in Information System Security • The e-Learning (SmartForce) modules in Internet Security. • The IASO course. • DISA's Operational Information System Security CD-ROM. • The e-Learning (SmartForce) modules in both Internet Security and Net Safety. • Other Service or commercial vendor courses.
4	Complete the ten day technical System Administrator/Network Manager Course (Level II) within six months of appointment and maintain a record of the completion date.
5	Complete/Attend one of the following every 18-24 months: • A four day Army IA workshop or a DOD sponsored IA workshop. • The e-Learning (SmartForce) modules Securing Networked Information I or Securing Networked Information II. • The e-Learning (SmartForce) modules Microsoft or UNIX or any Microsoft module. • Other Service or DOD IA workshops.

SCANNING AND REMEDIATION

F-47. The paragraphs below discuss scanning and remediation.

Scanning

F-48. Scanning is the gathering of information on information systems and device configurations, which may be used for system identification, maintenance, security assessment and investigation, vulnerability compliance, or compromise. This includes network port scanning and vulnerability scanning, whether wired or wireless, classified or unclassified. Scanning is conducted throughout all phases of operation (phases 0-4).

F-49. An operational scanning capability will be retained at the unit level as well as layered throughout the enterprise operational management structure for all classifications of networks. Regular, scheduled, and no-notice scans are integral to Security Policy and Compliance Enforcement and shall be done at all levels and all operational networks. Scanning tools may be obtained through Communications Security Logistics Activity.

F-50. Assessors must use a five-step methodology for assessment scanning as follows: identify assets, determine vulnerabilities, review vulnerabilities, remediate vulnerabilities, and validate remediation measures. All new information systems and device vulnerabilities must be proactively managed.

F-51. System administrators/Network managers must identify and prioritize which systems are most critical and develop a protection strategy. System administrators/Network managers and IA personnel will perform routine and scheduled unit vulnerability assessments and management in addition to IAVM procedures to manage system and network vulnerabilities proactively, and to maintain the necessary skill sets to remediate vulnerabilities proficiently, whether these networks reside with generating or deployed forces. Table F-6 details the actions that must be conducted when scanning.

Remediation

F-52. The system administrator/network manager will ensure the confidentiality of information by preventing unauthorized individuals access to computer equipment. The system administrator/network manager will patch system security vulnerabilities on all Army platforms. DOIM and tactical unit administrators are required to validate patches whether on the installation network or placed in storage. These requirements should be stated in unit OPORDs and other directives with command.

Table F-6. Scanning guidelines/actions

Step	*Scanning guidelines/actions*
1	System administrator will obtain and maintain training and certification on Army-approved IA scanning tools from Communications Security Logistics Activity located at https://informationassurance.us.army.mil/.
2	System administrator will review Army Best Business Practices at https://informationassurance.us.army.mil.
3	System administrator will scan network-attached devices with Army approved products monthly or after receipt of an IAVA.
4	System administrator will review scans report and determine devices to be patched. Update locally created database/spreadsheet for future reference on false positives.
5	IASO and system administrator will manually or electronically remediate devices requiring patch.
6	IASO and system administrator will rescan network for patch verification.
7	IASO and system administrator will maintain scan results locally and report scan results to the organization commander and IA personnel, DOIM and servicing NETCOM and information management area component, RCIO, functional CIO, RCERT/TNOSC, or ACERT/A-GNOSC.
8	IASO and system administrator will update A&VTR with compliancy information.

F-53. System administrators are responsible for reducing the vulnerability of their system through the application of software patches, both hot fixes and service packs. Table F-7 details the actions taken during the remediation process.

Table F-7. Remediation actions

Step	*Remediation actions*
1	Implement unit policy directing, on a weekly basis, users log off their work stations but leave work stations on for application of patches during non-duty hours. Specific day to be determined by unit IAM.
2	Receive IAVA identifying required patch.
3	Select required patches from the applicable Web site.
4	Ensure individual responsible for IAVM has administrative rights to the assets to be scanned and patched.
5	Scan assets (servers, routers, switches, and workstations) to identify assets that require patch application.
6	Identify “test” machine, apply patch, and scan the machine to confirm patch application.
7	Apply patch to the remainder of assets.
8	Issue Conformance Report (via patch application software).
9	Rescan to validate patch application.

Appendix G

Brigade Combat Team and Division Deployment Scenarios

During normal peacetime operations, the Army prepares its units for force projection missions. This requires organizing, training, equipping, and leading Army units to prepare them for force projection. Readiness and collective deployment training with Navy and US Air Force controlled lift assets is key in the force projection preparation.

PREDEPLOYMENT PHASE

G-1. During the predeployment phase, network planners must understand and plan for the complexity of joint, combined, and tactical network deployment and management needed to support the mission. They must have a clear understanding of the density of command post subscribers and automation networks in order to ensure that plans adequately meet requirements and facilitate proper network management. This requires adequate planning, engineering and support of the requisite nodes, transport links, STEP or teleport interfaces, network management centers, command and control relationships, and data management structures needed to support the theater network.

BRIGADE COMBAT TEAM AND DIVISION DEPLOYMENT EXCURSIONS

G-2. This section outlines the three base scenarios that support the Army providing forces to a CCDR: the BCT deploying alone, the BCT working directly for a joint headquarters, and several BCTs commanded and controlled by a division. There may be several branches or sequels to this deployment strategy, but the network has been designed to support these base capabilities required in the Army Comprehensive Guide to Modularity volume I version 1.0 (October 2004).

BRIGADE COMBAT TEAM WORKING FOR A FIXED JOINT HEADQUARTERS (EARLY ENTRY)

G-3. Once the Army is notified that a CCDR needs ARFOR, the initial fighting combat capability arrives in the form of the BCT. This BCT is a multicapable combat formation consisting of organic artillery, engineer, network, military intelligence, maneuver forces (Armor, mechanized infantry, or light infantry), and sustainment assets. These capabilities, combined with a multicapable brigade staff, enable the BCT to work directly for a joint headquarters if necessary.

G-4. An early entry BCT may be task organized under an Army-based command, such as a numbered Army acting as a JTF or JFLCC. Alternatively, a BCT may be task organized directly under a non-Army command, such as the geographical combatant command. In either case, the numbered Army provides supporting services that may be utilized by the BCT. Some of the supporting services include network service center regional termination, server sanctuary support, and theater support services. For example, as the BCT prepares for mobilization, the brigade S-6 prepositions a domain server, e-mail server, and VOIP call manager at the network service center regional. As BCT assets execute the reception, staging, onward movement, and integration and initial entry phases, they access these services via TDMA and FDMA links to the network service center regional. The BCT can also access tactical support services via the network service center regional; e.g., the numbered Army trouble ticketing system, storage services, and Web portal.

G-5. When the BCT deploys, the BCT S-6 coordinates with the CCDR higher headquarters J-6 and the local SC(T). The SC(T) is the primary network provider for theater LWN. It is also responsible for manning

and operating command and control of the Service TNOSC. The Service TNOSC performs the NETOPS functions for the Army theater assets, including the NETOPS interface with Army tactical communications formations. When the BCT falls directly under a non-Army command, the numbered Army SC(T) may also provide a liaison team to the BCT or joint command in order to facilitate operational communications. For example, if a BCT were to fall under the geographical combatant command, the TNCC may not have the necessary equipment to exchange data with the BCT. In this situation, the numbered Army may employ a liaison team to support the BCT. This team would provide any necessary data translation to the TNCC and ensure that the BCT receive the supporting and management services to which it is accustomed.

G-6. The BCT NOSC, as an integral part of the BCT signal company, will take all NETOPS directives from its higher headquarters' NOSC with the coordination and assistance from the BCT S-6. As the ARFOR, it also receives technical direction from the Service TNOSC. Additionally, the tactical formation will tie into the brigade on the Ku-band's TDMA using the strategic numbered Army brigade's UHN. The BCT signal company may also use existing Ground Mobile Forces or Secure Mobile Anti-Jam Reliable Tactical Terminals to tie into DISAs STEP sites or teleports. These fixed sites provide the SIPRNET, NIPRNET, video teleconferencing, and voice connectivity across the DISN. Figure G-1 shows the connectivity on a single BCT excursion.

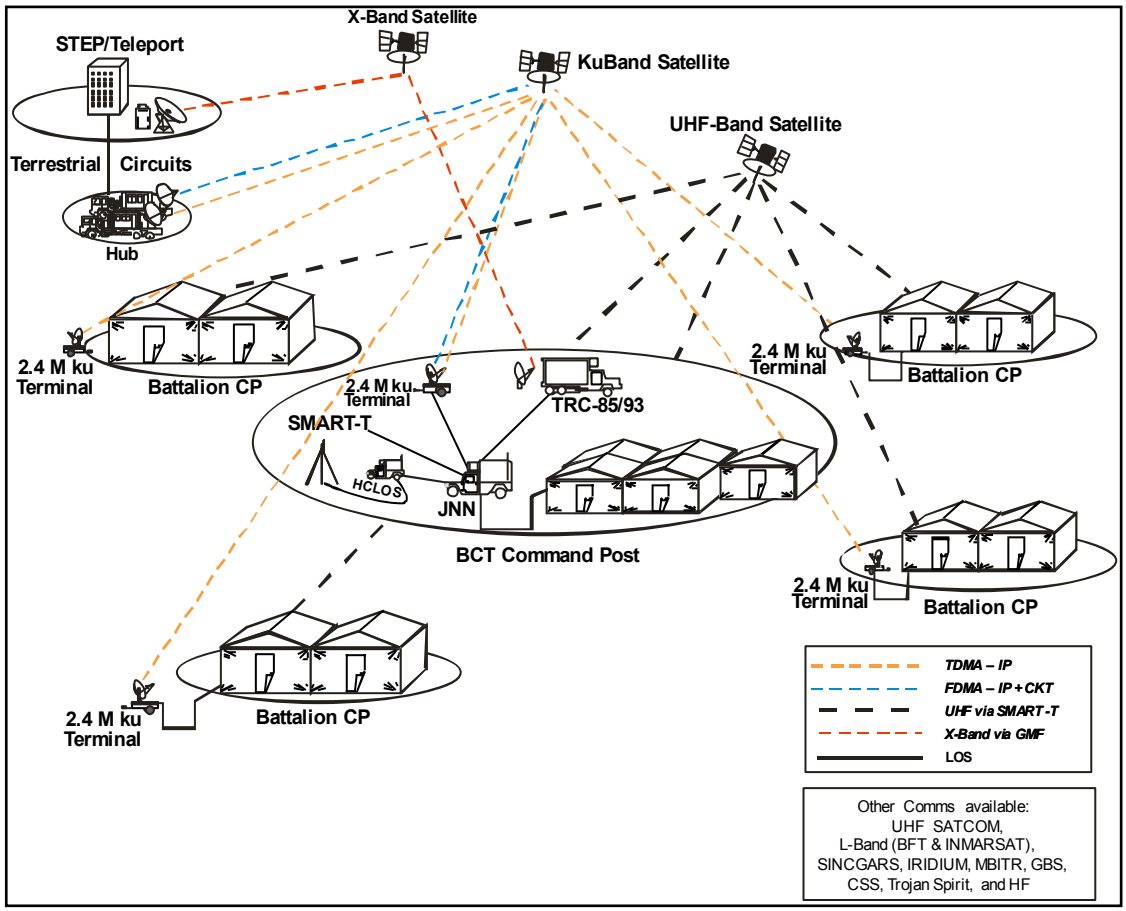

Figure G-1. The single BCT excursion

BRIGADE COMBAT TEAM DEPLOYING, WORKING DIRECTLY FOR A DEPLOYED JOINT HEADQUARTERS

G-7. The Army may be called upon to deploy the BCT in direct support of a deployed JTF, JFLCC, or other joint headquarters. This scenario requires that the BCT utilize the same communications procedures

used when deployed alone to connect to the GIG. The additional requirement for direct linkage to the joint headquarters may require an additional communications link. This link (non-Ku-band TDMA) can be accomplished with the organic Ku-band FDMA capability or organic Secure Mobile Anti-Jam Reliable Tactical Terminals. The e-mail or organizational messaging server (e.g., Defense Message System Groupware Server) will have to be commissioned into the DISA Defense Message System architecture if a corps, division, or numbered Army's Tactical Message System is not present. A redundant capability to the joint headquarters uses the GIG. Figure G-2 depicts BCT deployment connectivity.

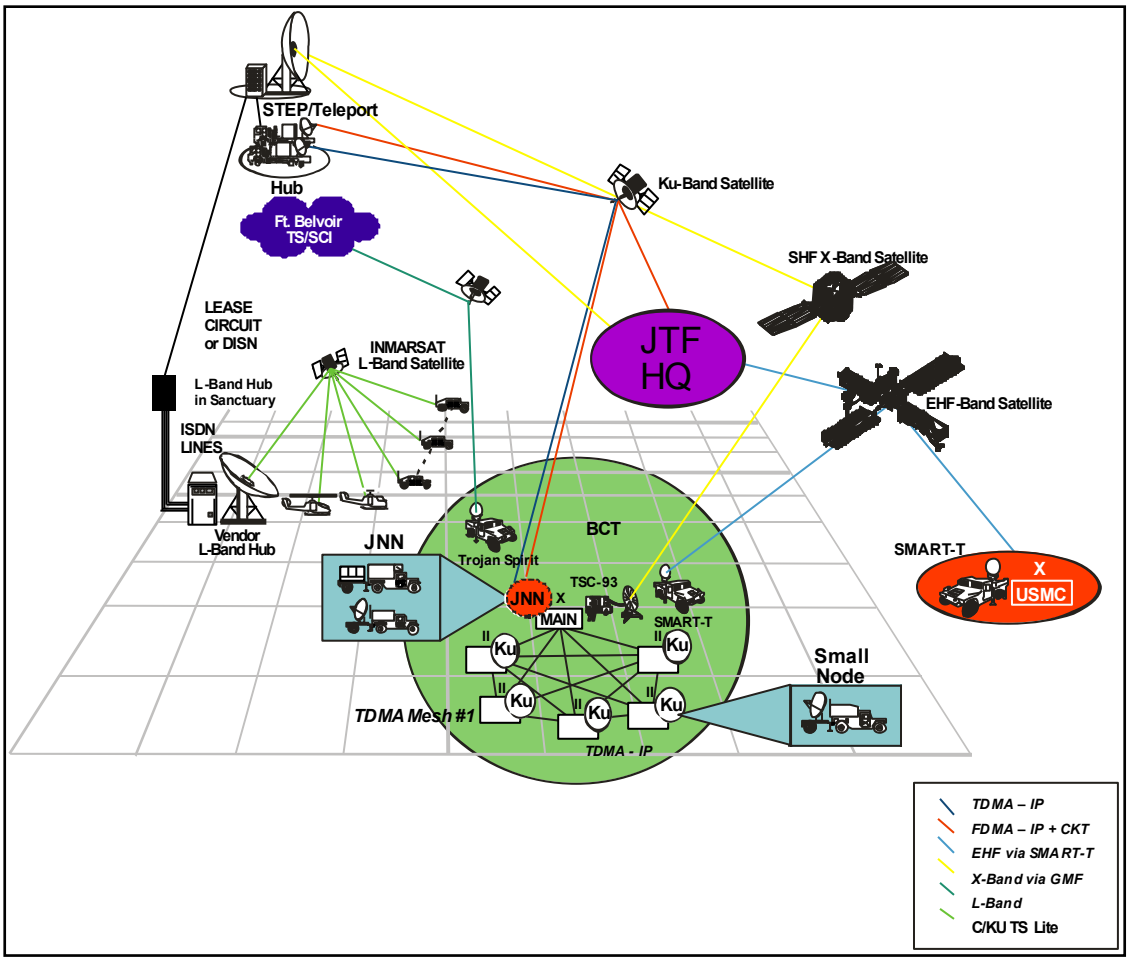

Figure G-2. BCT deployment connectivity

Division Deploying

G-8. The division headquarters may deploy with command and control of several brigade subordinates and possibly other Service land forces. If the division is given command and control of other Service land components, joint manning and network management equipment may be necessary. An example of network management equipment is the joint network management system which is not doctrinally allocated to division level forces.

G-9. In order to increase responsiveness of a complex network and to facilitate the bandwidth required to support the division and BCT networks, the division employs a NETOPS cell with the UHN. While the embedded NETOPS cell provides the management to enable the division network, the UHN flattens the disparate TDMA satellite network structure, and increases the bandwidth capability from approximately 6 Mbps to 40 Mbps.

G-10. In addition to expanding bandwidth, the division has the capability to dynamically reassign the bandwidth so that the communications support plan corresponds with the division commander's ground tactical plan. The division weighs one BCT as the main effort for an assault. As the main effort, the division commander gives the BCT a direct unmanned aerial vehicle or sensor feed that needs to be broadcasted across the network. The division G-6 can match the communications support plan to enable the added, non-organic capability. This process is achieved by allocating a larger slice of the division enabled 40 Mbps of bandwidth when the capability is required. The division hub provides an unprecedented capability that quickly "squirts" capabilities to those who need it in order to enable the ground tactical plan.

G-11. The division may also use the network service center regional in lieu of or in addition to the division UHN network service center deployed. The network service center regional provides a persistent hub and NETOPS capability in support of the division when the network service center deployed, is unavailable, oversubscribed, or malfunctioning.

G-12. The NETOPS cell, ICW the network hub, links capabilities to network governance or management. The NETOPS cell performs management as an extension of the GIG's strategic management, yet the tactical cell responds to priorities of the division tactical plan. Figure G-3 depicts the division deployed.

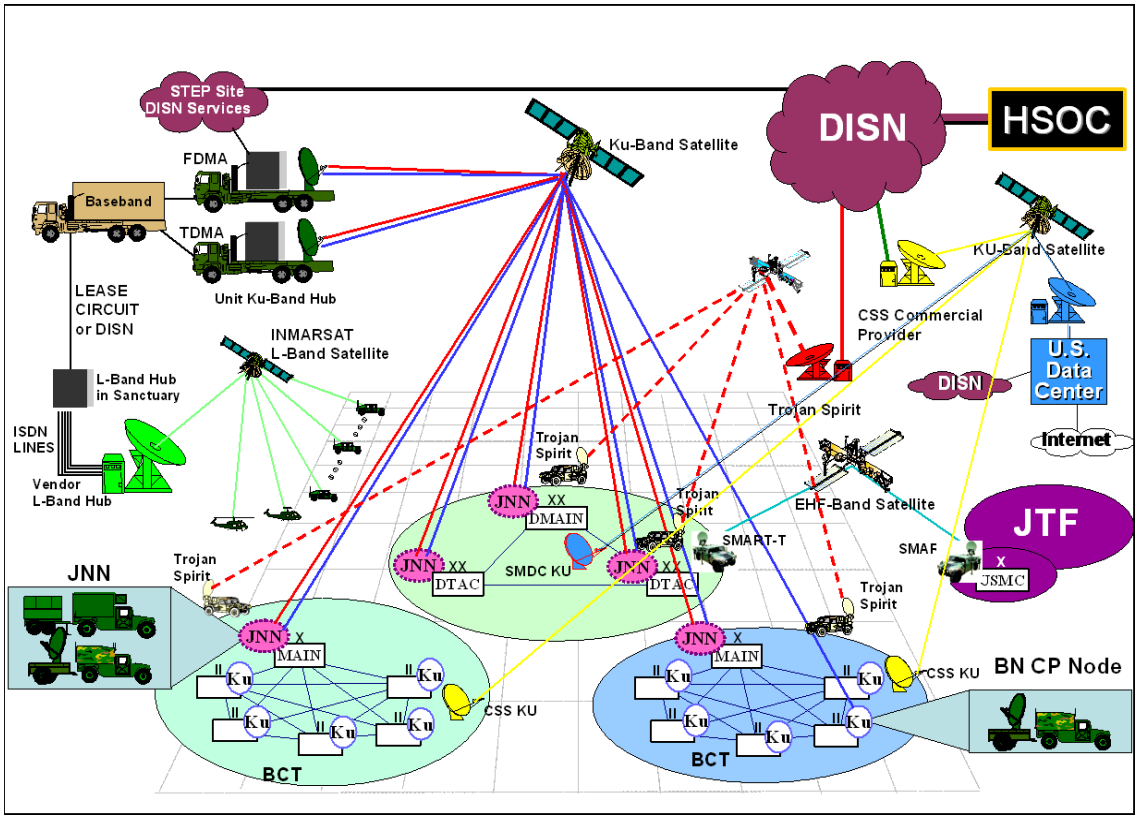

Figure G-3. Division deployed

Appendix H

Numbered Army Operational Scenarios

In order to illustrate the various roles and responsibilities of the numbered Army in an operational environment, it is necessary to analyze the likely scenarios in which the numbered Army would play a critical role. These scenarios drive the discussion behind the command and control relationships of the different commands across the phases of operation, as well as the functions performed by the various NETOPS personnel. Before we can review the detailed NETOPS functions associated by phase, it is necessary to describe the NETOPS scenario along with the corresponding command and control relationships.

OVERVIEW

H-1. The following sections will illustrate three common operational scenarios. The first scenario is comprised of two BCTs that fall under the command of a numbered Army-based JTF. The second scenario involves a major combat operation in which the numbered Army acts as the JFLCC and commands several division units. The final scenario depicts a major combat operation scenario in which a numbered Army-based JTF has been designated as the JTF for the joint operational area. The supporting and commercialization services are provided by the numbered Army as the ASCC. As a joint operation progresses, it will pass through one or more of these scenarios in a sequential fashion.

SCENARIO 1: EARLY ENTRY OPERATIONS

H-2. In this scenario, the US Northern Command CCDR has received direction from the CJCS to rotate units into a theater of operation to relieve an existing Army force. Based on the time phased force deployment data, US Northern Command directs their numbered Army (FORSCOM) to provide forces which results in the selection by the Northern Command numbered Army of two BCTs. This force will serve under a numbered Army-based JTF in the gaining theater.

H-3. Once the BCTs are notified of the deployment order, the BCT staff begins deployment planning through the combined processes defined in the joint planning process (JP 5.0 Series) and the Army's military decision making process. The joint planning process may include any combination of commands based on the mission. At a minimum, the BCT S-6 will need to conduct joint planning with the JTF J-6, Service TNOSC in theater, and potentially CONUS based entities that influence the BCT mission under the JTF.

H-4. The numbered Army, within the operational theater, may execute its role of JTF in several different formations. The numbered Army may be "dual-hatted" as the JTF and simply assume the responsibilities of the JTF in addition to its habitual ASCC responsibilities. Alternatively, the numbered Army may designate a portion of its assets to act as the JTF and these assets may or may not be required to deploy forward into the operational environment. For the purposes of this scenario, we will assume that the numbered Army has sufficient connectivity into the tactical environment to enable it to perform its mission from a location within the fixed-station. JTF J-6 functions are performed by a designated portion of the SC(T). JTF NOSC functions are performed by the TNT within the TNOSC. The SC(T) and TNT perform all JTF and ARFOR functions, in addition to all NETOPS functions that would typically be performed by a division when one is present. This allows the BCTs to function in a fully modular and standardized manner.

SCENARIO 2: MAJOR COMBAT OPERATIONS

H-5. If the combat operation described above escalates and requires the deployment of additional Army forces, one or more divisions and additional BCTs and support brigades will be mobilized. In the event of a small operation of this type, the geographical combatant command may designate a corps or division to act as the ARFOR. The corps or division acting as an ARFOR is detailed in Appendix D. For the purposes of this scenario, we will assume that the geographical combatant command chooses to assume direct control of the operation, and delegate's control of land forces to the local numbered Army. The numbered Army is then "dual-hatted" as the JFLCC.

H-6. As the size of the operation grows, additional assets will be required at the SC(T) and TNT to command and control the operational area. These assets can be drawn from the numbered Army organizations in other theaters. For example, when a corps or division deploys from CONUS, a portion of the CONUS TNOSC TNT may also be required to deploy in support of the gaining TNT.

H-7. When the numbered Army is designated to form the basis of a JFLCC, the SC(T) is required to provide user services and integrate deployed, unit-owned services in support of the JFLCC AOR. For example, the SC(T) would provide central video teleconferencing hub services, inter-unit VOIP routing services, domain synchronization, and central storage services. The SC(T) generally delegates this mission to the SB(T). The signal brigade (theater) may perform these functions from either the network service center regional or the signal brigade (theater) systems control. The signal brigade (theater) may require augmentation from signal brigade (theater)s in other theaters in order to provide common user services for the JFLCC AOR, in addition to the habitual signal brigade (theater) responsibility of providing basic user services for ITSB/ESB-supported assets.

H-8. The gaining SC(T) provides various supporting services to the corps or division as it enters the theater. This is a responsibility of the SC(T) regardless of whether the numbered Army has been designated to act as a member of the operational chain of command. The SC(T) allocates satellite and DISN services for corps or division use and provides a sanctuary environment at the network service center regional for corps or division NETOPS services. The local TIC within the TNOSC ensures that the corps or division network management systems are synchronized with higher headquarters management systems. These systems include trouble ticketing systems, IA event correlation systems, and network monitoring systems. To perform these missions, the TIC will typically form a liaison team to augment the corps or division NETOPS personnel within the UHN or network service center regional.

H-9. The numbered Army, as the JFLCC, may be required to deploy the numbered Army command post to command and control the joint operational area. This command post is provided with basic network services via ITSB/ESB signal assets. The command post will also require support from the TNT to provide SA and to interface with the JFLCC command and staff. The bulk of JFLCC NOSC functions should be performed from the service TNOSC whenever possible in order to reduce operational environment transmission requirements and simplify service architecture.

H-10. In a major combat operation, regardless of the operational role of the numbered Army, the SC(T) will be required to deploy ITSB/ESB assets to support operational environment organizations that may not have organic signal support. This includes numbered Army-based command posts, certain support brigades, ports of debarkation, coalition forces, and non-military agencies. ITSB/ESBs that are supporting corps or division assets, such as a support brigade that is under the OPCON of the corps or division, fall under the command and control of the corps or division G-6. ITSB/ESBs that support numbered Army or JFLCC assets fall under the command and control of the signal brigade (theater).

H-11. In major combat operations, a corps or division may become an intermediate tactical headquarters under the command of the JFLCC. Complexity, span of command, or multinational considerations may require the use of a third controlling echelon above the brigades. When this occurs, the corps or division G-6 may require additional augmentation from numbered Army signal brigade (theater) or TNT assets to perform its mission. As the major combat operation transitions to protracted stability operations, the additional corps or division headquarters returns to its home station and the normal two-echelon arrangement will remain.

SCENARIO 3: PROTRACTED STABILITY OPERATIONS SCENARIO

H-12. As a major combat operation transitions to protracted stability operations, the geographical combatant command may require the numbered Army to form the basis of a JTF to control the joint operational area. For this scenario, we will assume that the numbered Army will no longer act as a "dual-hatted" command, but will establish a separate command to control the joint operational area.

H-13. When the numbered Army-based joint operational command is separated from the numbered Army ASCC, command and management authorities are divided accordingly. The portion of the SC(T) which is performing ASCC functions acts solely in a support role, while the portion of the SC(T) which augments the joint command has OPCON of the network operational environment. For example, the deployment support division within the TNOSC assumes the responsibilities of providing NOSC functions to the joint command. It is likely that the deployment support division will require pooled assets from other theaters to perform this function in a major combat operation. The remainder of the TNOSC performs a purely ASCC function by providing value added and title-10 functions in support of the joint command.

H-14. ITSB/ESB assets which support elements of the joint operational command fall under the command and control of the joint command. In a large major combat operation scenario, the numbered Army signal brigade (theater) may be dedicated to the support of the joint command in order to provide a span of command for the ITSB/ESB units within a joint operational area.

Appendix I

Fixed Regional Hub Node Operations and Control Plan

The Joint Network Node-Network (JNN-N) hub nodes are critical elements of the new JNN-N family of equipment that supports commercial Ku-band SATCOM. In the future, the JNN-N network will also operate off of the Wideband Gapfiller Satellite constellation. This appendix identifies the roles and responsibilities of the fixed regional hub node (FRHN), the mobile regional hub node (MRHN), the tactical hub node (THN), the Training Hub Node and describes the services provided via these nodes. This appendix will concentrate on the FRHN and the MRHN, and provide a foundation for the interface to APCs and the migration to the network service center-regional concept. In addition, this appendix will discuss the FRHN Operations and Control Plan. The FRHN Operations and Control Plan outlines the procedures for JNN-N enabled/compatible units to request services from the FRHN. This manual does not specifically address support for other services, e.g., Army-Marine Corps Memorandum of Agreement, nor does it specifically address the CCDR's use of FRHNs. Rather, it is focused on the roles and responsibilities within the processes and procedures necessary for the Army to effectively support the CCDR. It is envisioned that the processes and procedures outlined in this document can be adjusted to support Joint missions once memorandum of agreements are established with the other services interested in utilizing the FRHN.

FIXED REGIONAL HUB NODE

JOINT NETWORK NODE-NETWORK HUB NODE'S ROLE IN THE OBJECTIVE TACTICAL ARCHITECTURE

I-1. The JNN-N architecture is one of several emerging and interdependent initiatives to move towards the objective tactical Army network architecture (refer to FMI 6-02.60). The JNN-N hub node also plays a key role in the TRADOC Program Integration Office's network service center-regional and the CIO/G-6 APC constructs. These related initiatives will not be addressed in any detail within this manual. However, they are described briefly in order to ensure that the JNN-N hub nodes responsibilities and functions within the near term and objective environments are clearly understood.

NETWORK SERVICE CENTER-REGIONAL

I-2. The network service center-regional concept addresses the Soldier requirement for ubiquitous, standardized, and modular service support across the globe. The network service center-regional is a collection of standardized capabilities which will be physically realized via several disparate facilities and organizations. While initial network service center-regional capabilities will be Army-focused, the objective network service center-regional is a joint capability, and would provide standard services to any tactical unit as defined by joint guidance.

AREA PROCESSING CENTER

I-3. Under the APC construct, tactical, area, regional, and enterprise services are delivered from a centralized location in a standardized manner above the post/camp/station, i.e. installation, level. An APC will be a concentration point for installation interconnectivity, and a location for common services. This concept will provide a standardized approach to facilitate LWN intranetwork communications and provide a service delivery paradigm by mission or functional community instead of geographic boundaries. For example, it will be feasible for Solders to position battle command applications at the APC for primary or backup services in support of their deployed forces.

JNN-N HUB NODE INTEGRATION WITH THE NETWORK SERVICE CENTER-REGIONAL AND AREA PROCESSING CENTER

I-4. The APC and JNN-N hub node are two of several physical entities that will ultimately contribute to the combined network service center-regional capability. In theaters where an APC is not yet present or fully functional, services may be staged within the FRHN. As the APCs are built, tactical area services will be migrated to the APC. The APCs will be sized to accommodate additional services and provide data replication capabilities to facilitate garrison-to-tactical deployment transitions.

TNOSC INTEGRATION WITH THE NETWORK SERVICE CENTER-REGIONAL

I-5. While the FRHN provides the transport and the APC provides data center services, the TNOSC will provide the NETOPS for the network service center-regional and APC. The TNOSC NETOPS capability will ensure transport and data center resources are available, reliable, and secure to meet the Solder's operational requirements. The TNOSC will be responsible for integrating with other Army and joint network operations centers (NOCs) and NOSCs, both vertically and horizontally, to gather and report NETOPS and SA data. The TNOSCs will report vertically to the A-GNOSC, which has Army Enterprise Management oversight.

JOINT NETWORK NODE-NETWORK HUB NODE'S ROLE IN WARFIGTER INFORMATION NETWORK-TACTICAL MIGRATION STRATEGY

I-6. The JNN-N hub node concept plays a critical role in the Army's migration to the Warfighter Information Network-Tactical network. As a centralized operational base (strategic) support node to tactical assets, the JNN-N hub node facilitates the projected migration to a network architecture with ubiquitous low latency access to operational base (strategic) services and begins the transformation from the current "federation of networks" to an integrated network service provisioning and management paradigm. The Army CIO/G-6 has developed a comprehensive plan to synchronize JNN to Warfighter Information Network-Tactical acquisition through fielding implementations.

JOINT NETWORK NODE-NETWORK HUB NODE TYPES

I-7. The paragraphs below discuss the four types of JNN-N hub nodes: FRHN, MRHN, THN, and the Training Hub Node.

FIXED REGIONAL HUB NODE

I-8. Five FRHNs will be deployed at fixed operational base (strategic) locations in order to provide near worldwide coverage. FRHNs will allow satellite, voice, and data services to be provisioned and pre-positioned to support deploying forces as they flow into a theater of operation. FRHNs will be located in the European, Southwest Asia, and Pacific OCONUS theaters, as well as the CONUS East and West Coasts. The first FRHN is expected to be operational in Southwest Asia in fiscal year 08. The FRHN is the largest of the four JNN-N hub node types, and has the following capabilities:

- Provides primary hub node connectivity FDMA and TDMA and services for tactical users during reception, staging, onward movement, and integration operations.
- Provides TDMA management support enabling intra-theater brigade-to-brigade level routing and network services.
- Provides COOP for MRHNs and THNs.
- Provides primary hub node connectivity and services to expeditionary units (e.g., BCT) not deploying with a THN.
- Provides support to ESBs/ITSBs that are task organized to support all echelons.
- Provides a server sanctuary supporting the delivery of theater level services and a stable location for division or brigade units to host services for their tactical users.
- Provides JNN-N hub node connectivity and services for mounted battle command on the move users.
- Supports up to three JNN-N-equipped divisions, or is reconfigurable to support two JNN-N equipped divisions, four BCTs, and one separate (non-BCT) mission.
- Extends DISN voice, data, and video services to the Solders.
- Provides assured, low latency connection and reach to the TNCCs for Top Secret/Sensitive Compartmented Information (TS/SCI) users using JNNs or CPNs as their transport connection to the FRHN.

Note. For the purpose of this manual, ESBs ITSB are synonymous. An approved doctrinal naming convention is pending.

I-9. The FRHN can be divided logically into three subcomponents: SATCOM, baseband services, and NETOPS and user services. Each FRHN is co-located with a DOD Gateway, which enables cost savings by sharing common infrastructure (e.g., power, heating, ventilation, and air conditioning) and access to the DISN infrastructure. The DISA Earth Terminal (part of the DOD Gateway) facility houses all FRHN devices that require physical proximity to satellite and baseband equipment, and will be operated and maintained on a 24 hours a day, seven days a week basis. Initially, the operations and maintenance personnel for the FRHN will be contractors (approximately 17 personnel), which is an interim capability until such time as a BOIP is approved and applied towards Table of Organization and Equipment/Modified Table of Organization and Equipment. Co-location with a DOD Gateway enables the extension of DISA services to warfighting units and high bandwidth connectivity into the GIG.

I-10. For FRHN operations, the program manager for Defense Communications and Army Transmission Systems (DCATS) will install three large, high-bandwidth, multi-carrier satellite terminals. These satellite terminals will be operated and maintained by the FRHN SATCOM personnel as identified in the FRHN BOIP. Based on commercial satellite licensing requirements, civilian contractors holding commercial licenses will be utilized to operate and maintain the commercial satellite subsystems of the FRHN. The commercial contractors will coordinate any OCONUS host nation approvals/foreign government licensing requirements and CONUS Federal Communications Commission licensing requirements that are required to operate the terminals. The NETOPS management and user services will be hosted on the same installation as the FRHN, and initially will be supported by FRHN NETOPS personnel as identified in the BOIP.

MOBILE REGIONAL HUB NODE

I-11. The MRHN is a transportable hub terminal that operates from a sanctuary location. The MRHN is intended to:

- Provide coverage in areas where an FRHN has not been built or has no coverage.
- Provide hub node connectivity to expeditionary units (e.g., BCTs) not deploying with a THN.
- Supplement an FRHN when additional capacity or satellite coverage is required.

- Provide TDMA management support enabling intra-theater brigade-to-brigade level routing and network services.
- Provide a termination capability for mounted battle command on the move terminals.
- Provide unit sustainment training and exercise support.
- Support autonomous BCTs operating independent of a THN supported division.
- Support ESB/ITSB TDMA and FDMA based command posts.

I-12. The theater level tactical MRHN consists of two mobile SATCOM shelters and a mobile baseband shelter. The MRHNs will be operated and maintained by a theater strategic signal brigade IAW an approved BOIP. The MRHN is capable of interfacing with DISN points of presence and legacy Army signal systems (e.g., mobile subscriber equipment, tri-services tactical, and ground mobile forces satellite terminals). There are currently two first-generation THN terminals which will become the MRHN nodes. These terminals were originally fielded to the 3ID for Operation Iraqi Freedom 3, and will be transitioned to NETCOM at a time to be determined. Once 3ID is fielded with the newest generation of THN being built on the family of medium tactical vehicles, the original two hubs will be assigned to NETCOM to support restoral and contingency missions. No further acquisition of MRHNs is currently planned. The MRHN manning structure under NETCOM will be consistent with the approved BOIP. MRHN assets will be pooled and may be allocated to the various Army theaters as requirements are identified.

TACTICAL HUB NODE

I-13. The THN will be used for direct support to the division and its subordinate units. It provides the following capabilities:

- Primary hub node support to a division and its subordinate units.
- TDMA management support enabling intra-theater brigade-to-brigade level routing and network services.
- Service delivery point for division level services and applications.
- Termination capability for mounted battle command on the move terminals.
- Capability to operate in a sanctuary location w/DISN point of presence access, wherever possible.
- Division level training hub.

I-14. The THN consists of two mobile SATCOM shelters and a mobile baseband shelter. Operations and maintenance will be IAW the current THN BOIP. The baseband assemblage is capable of interfacing with a DISN point of presence and legacy (as with the MRHN) Army Signal systems. The current fielding plan is one THN per Army division.

TRAINING HUB NODE

I-15. The Training Hub Node is currently located at the US Army Signal Center, Ft. Gordon, Georgia. The Training Hub has capabilities similar to a THN; however, the baseband equipment is located inside a fixed facility. The Training Hub's primary purpose is formal school house training to prepare Soldiers to operate, manage, and interface with JNN-N assets. However, the Training Hub is currently supporting training readiness exercises, mission rehearsal exercises, etc. until the CONUS FRHNs are fielded and operational. Once the CONUS FRHNs are fielded, the Training Hub will primarily support school house training and be available for strategic reserve to support Homeland Defense, Homeland Security, and other CONUS/US missions. The Training Hub Node will also be used to develop JNN-N hub node doctrine, training, force structure, and SOPs. The Training Hub Node will transition into a larger Network Service Center-Training capability in the future when APC and TNOSC capabilities are integrated.

JOINT NETWORK NODE-NETWORK SERVICES CAPABILITIES

I-16. A service is a package of one or more related capabilities or functions that provide value to a customer. This section will describe a set of services which will be provided by or accessible via any JNN-N hub node.

I-17. Due to their mobile nature, the MRHN and THN may not provide the full suite of services at the hub node site. Services that are not provided at the MRHN or THN location would be provided remotely from other locations, such as an FRHN, DOD Gateway, APC, and/or TNOSC. The placement of services supporting MRHN or THN users is dependent upon unique theater and operational factors, and will be determined by the unit or organization with operational control of the service.

I-18. The exact location of FRHN services within each theater will also be determined by the unique architecture and resources of the theater. For the purposes of this document, the FRHN will consist of a Services Facility and Communications Facility. The FRHN Communications Facility will house the satellite intermediate frequency equipment and the baseband communications equipment. It is envisioned that the Communications Facility will co-locate and occupy floor space inside the DOD Gateway Earth Terminal Complex. The Communications Facility will be manned with personnel from the theater strategic signal brigade.

I-19. Liaison personnel from the supported tactical units will deploy to the FRHN to assist with the initial configuration of Tier 2 equipment that interfaces with their deployed forces, as dictated by mission requirements. The liaisons will also facilitate NETOPS and troubleshooting issues between the FRHN and deployed force personnel. Ideally, a liaison presence will remain at the FRHN throughout the duration of their operation. However, deployed force mission requirements may prevent a full-time presence at the FRHN. For example, if the primary hub node supporting the deployed force transitions from the FRHN to a THN (when it arrive in-theater), the liaison personnel will likely transfer to the THN, and the FRHN will become a backup capability for the deployed force.

I-20. Deployed force technicians could then remotely access Tier 2 devices inside the FRHN, as required. During the initial phases of an operation, it is critical that the deployed force S-6/G-6 coordinate with the theater signal brigade S-3 to define liaison support activities at the FRHN. Tier 2 equipment configurations must be well understood by liaison and FRHN personnel to ensure tactical units can successfully integrate into the FRHN. Liaison and deployed force personnel will have local and remote access capabilities to Tier 2 equipment that includes routers, switches, call managers, and NETOPS servers. Any Tier 2 application servers installed at the FRHN will be configured and managed by the division and BCT liaison officer (LNO) teams.

I-21. The FRHN Services Facility should not reside on the Communications Facility floor, but could reside in the same building or an adjacent building interconnected with high bandwidth assured connectivity. However, this may not be achievable at every FRHN location. The Services Facility is envisioned to house NETOPS management, common user, and functional area business servers, at both the UNCLASSIFIED and SECRET levels. At this time, it is not anticipated that the JNN-N hub nodes will provide any services above the SECRET classification level. However, encrypted data above the SECRET level, such as TS/SCI traffic, will tunnel through a JNN-N hub node to be decrypted at other locations.

I-22. FRHN Services Facility operators will be responsible for the operation and maintenance of Tier 1 NETOPS servers at the FRHN Services Facility which provide shared or theater-level services. Liaison personnel from the deployed tactical units will assist the Services Facility personnel with the configuration of Tier 2 devices, which include routers, switches, call managers, and NETOPS servers ESM/NM and IA/CND. Liaison or deployed force personnel are responsible for the configuration and operation of any Tier 2 application servers placed at the FRHN. During initial deployment, liaison personnel are expected to have the technical skills to configure their assigned Tier 2 equipment.

I-23. The FRHN Services Facility is also supported remotely by the TNOSC. The TNOSC has technical authority over the FRHN Services Facility. Figure I-1 is a simplified block diagram showing the

relationship of a CONUS FRHN to the TNOSC. Figure I-2 is a block diagram showing the relationship of an OCONUS FRHN to the TNOSC.

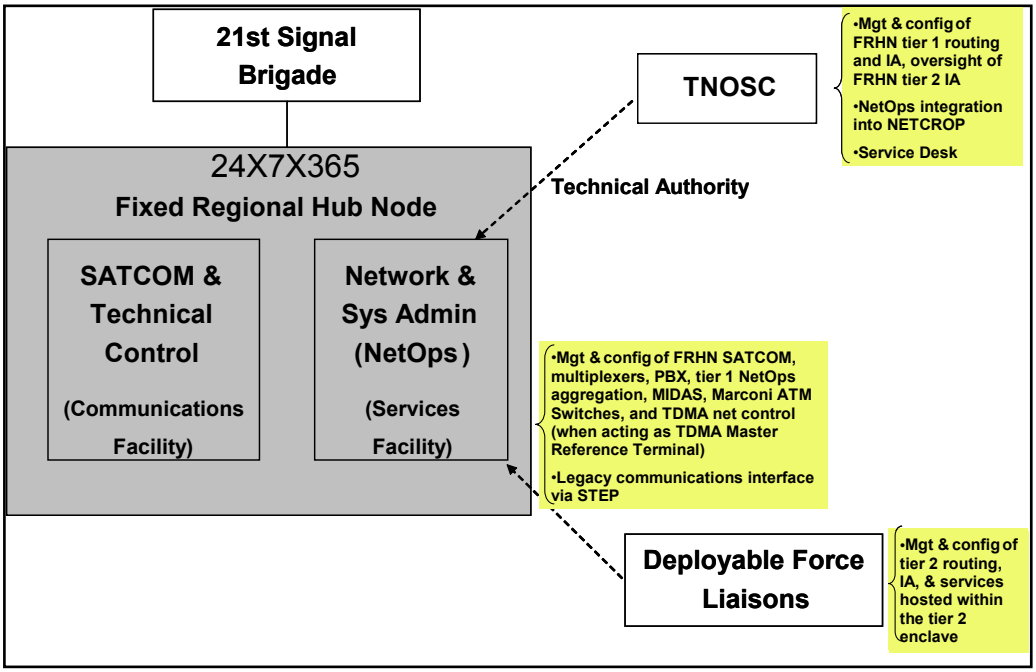

Figure I-1. CONUS FRHN/TNOSC relationship

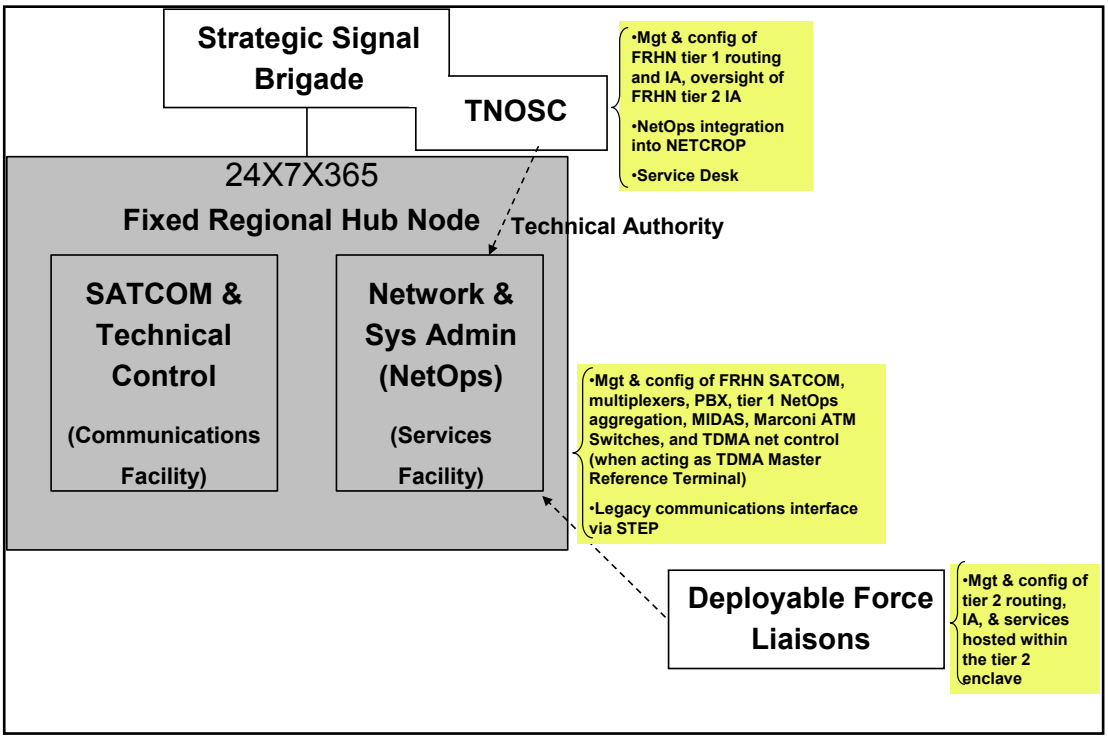

Figure I-2. OCONUS FRHN/TNOSC relationship

I-24. For TS/SCI services tunneled through the JNN-N, the FRHN will ensure the transmission path is operational from the hub node to the deployed JNN or CPN. The TS/SCI users are responsible for the proper configuration of their encryption, decryption and terminal equipment to ensure end-to-end system connectivity. The help desks located at the TNCCs will provide TS/SCI network management support to intelligence users. The FRHN locations must have network connectivity to the TNCCs in order to assure these TS/SCI users get the required quality of service, as well as connectivity to the wide area services not available at the DOD Gateway locations.

I-25. The TNOSC might not be co-located with the FRHNs. However, high-bandwidth and robust NIPRNET and SIPRNET connectivity via the DISN is required between the two facilities. The FRHN Services Facility will provide aggregated NETOPS data to the TNOSC for integration into the theater network common relevant operational picture. The TNOSC will also provide technical support to the Services Facility NETOPS personnel and provide NETOPS support for some Tier 1 and IA services in the FRHN and other deployed force locations.

PLANNING AND ENGINEERING

I-26. Communications planning and engineering shall be performed at all echelons. The SC(T) will have the overall responsibility for planning and engineering new missions into the FRHN and MRHN. For JNN-N equipped units that will be interfacing with theater Army assets (e.g., FRHN), requirements such as communications architecture and space segment requirements will be consolidated by the SC(T). The SC(T) will coordinate with supported unit G-6/S-6 representatives to complete an integrated theater JNN-N architecture. The SC(T) will coordinate the architecture with the supported JTF J-6. The SC(T) will also coordinate space segment requirements directly with the regional satellite support center (RSSC) or via the JTF J-6, as appropriate. The SC(T) will coordinate with the FRHN staff and TNOSC to perform detailed engineering of the legacy baseband systems and IA and IP transport, respectively.

DISN SERVICES

I-27. One of the primary roles of the JNN-N hub nodes is extending the GIG services to the Soldier. The FRHN interfaces with Army Tier 1/1 routers for the extension of DISN IP services. Non-IP services (e.g., DSN) are extended directly from the DOD Gateway. It is expected that the MRHN and THN will also be co-located with a DISN point of presence and provide the following services to the tactical users:

- NIPRNET.
- SIPRNET.
- DSN.
- DRSN.
- DISN video services.

I-28. The FRHN will be configured to provide two DRSN circuits per division enclave (via the FDMA/Promina network links). The DISN Video Services-Global is expected to have completed the migration from H.320 serial connectivity to H.323 IP connectivity by the time the first FRHN is operational. Therefore, serial circuits will not be planned or provisioned for H.320 based DISN Video Services-Global service. The IP-based DISN Video Services-II will be carried over the NIPRNET and SIPRNET links.

I-29. The FRHN will not decrypt or breakout Joint Worldwide Intelligence Communications System. Any Joint Worldwide Intelligence Communications System traffic will pass through the FRHN in encrypted format. It would then be routed via a tunneled connection over an available IP network or extended via a dedicated DISN connection to the appropriate operating facility. It is technically feasible to decrypt or breakout coalition traffic at the FRHN, as driven by theater ASCC requirements.

I-30. The MRHN and THN may or may not have terrestrial connectivity to a DISN point of presence. Several factors must be taken into account by commanders and signal planners regarding the best location for a MRHN and/or THN. The amount of time available for mission planning and the required proximity of

the JNN-N hub node to the Soldier may result in tradeoffs where DISN connectivity is not available at the start of an operation, if at all. Ideally, all deployed JNN-N hub nodes will have direct terrestrial DISN connectivity for redundant and robust communications. However, at a minimum, the FRHN will be DISN connected.

BASEBAND SERVICES

I-31. The MRHN and THN have a separate baseband shelter which provides baseband services, while the FRHN integrates these services inside a DOD Gateway Earth Terminal Complex. Services provided include:

- Multiplexing.
- Link encryption (e.g., KIV-19A and KIV-7HSB).
- IP encryption (e.g., KG-175).
- Patch and test.
- Private branch exchange phone service with DSN connectivity.
- Tier 1/2 NIPRNET and SIPRNET routing services.
- Tier 2 NIPRNET and SIPRNET routing services.
- IA services (e.g., intrusion detection, firewall, and deep packet inspection).
- VOIP.
- Secure VOIP.

I-32. Satellite and baseband planning and engineering shall be performed at all echelons. For JNN-N equipped units that will be interfacing with theater Army assets (e.g., FRHN), baseband service and space segment requirements will be consolidated through the operational chain(s) of command and communicated to the ASCC G-6 and SC(T). The prioritization and deconfliction of theater resource allocation ultimately resides with the GCC. The FRHN personnel will have the responsibility to coordinate with SC(T), JTF J-6, and supported unit G-6/S-6 representatives to engineer an integrated theater JNN-N architecture. The SC(T) will also coordinate space segment requirements directly with the DISA RSSC, GCC J-6, or via the JTF J-6, as appropriate.

SATELLITE TERMINAL SERVICES

I-33. At the FRHN, the antennas, radio frequency equipment, and a portion of the intermediate frequency equipment will be located outside of the Communications Facility. This equipment will be located inside an environmentally controlled shelter that is located in close proximity to the antennas. The equipment will be operated, maintained, configured, and managed by the Communications Facility personnel IAW the FRHN BOIP.

I-34. The L-band intermediate frequency will be transported from the satellite terminal equipment to the Communications Facility via fiber optic modems. The L-band interfaces from each terminal will terminate on L-band combiners and dividers inside the DISA Earth Terminal facility. L-band patch panels provide the interface to the TDMA, FDMA, and mounted battle command on the move satellite modems. This equipment will also be operated and maintained by the Communications Facility personnel. The SATCOM shelters at the MRHN and THN will be operated, maintained, configured, and managed by the Theater MRHN Team and the division signal company, respectively.

I-35. Master reference terminals are TDMA satellite modems that interface with the NCCs to provide timing and control for the TDMA network. The master reference terminals are under the OPCON of the Communications Facility at the FRHN, ITSB/ESB at the MRHN, and the division signal company at the THN. Each master reference terminal fielded is also fielded with an alternate master reference terminal. The current TDMA satellite implementation allows an automatic failover capability from a master reference terminal to an alternate master reference terminal, if the two devices are co-located on the same network segment. The automatic failover option will be enabled for all operational master reference terminals. In the

event that the entire node (e.g., THN) becomes inoperable, it is possible to manually failover to a remote node (e.g., FRHN). However the manual cutover will incur TDMA network downtime.

I-36. The FRHN will participate in all TDMA networks that are operating in-theater, assuming resources are available. Resources may not be available if additional missions are supported off the FRHN, such as support for autonomous BCTs, functional user support, or ESB/ITSBs not operationally controlled by a division. The FRHN has the capability to provide the primary master reference terminal/network control center (NCC) functionality for all TDMA networks. As units prepare and then deploy into the theater, the FRHN will provide the primary master reference terminal functionality. This ensures that satellite carriers are operational and waiting for the units as they arrive in theater. Having the primary master reference terminal/NCC functionality initially at the FRHN allows units at all echelons to join and leave the TDMA network in an ad hoc manner, which is ideally suited for a dynamic battlefield. As the TDMA network stabilizes, primary master reference terminal/NCC control for carriers assigned to the division can transition to the THN. However, due to satellite vendor equipment limitations, this requires a manual configuration and cutover process, which will incur downtime.

I-37. The DISA Teleport Generation II design will support "current force" modems (for example, Linkway and iDirect) in the near future (i.e., fiscal year 07–fiscal year 08). DISA supported current force modems do not replace the FRHN modems operated by the Army, but provide an increased pool of modems available that the Army may be able to leverage to meet operational requirements. The current force modems will operate on DISA terminals and require appropriate DISA SAR procedures to gain access. While Teleport Generation II provides TDMA and FDMA capabilities, FRHNs are required to ensure modular Army forces are provided with assured satellite access. Hub node personnel must also be responsive to deployed force network management and reallocation needs IAW the tactical commander's requirements. The hub nodes also support the deployed forces' need for intra-theater Tier 1 and Tier 2 networking and applications services.

I-38. ESBs/ITSBs supporting a division formation will interface with Tier 2 division enclaves at the THN, MRHN, and/or FRHN. ESB/ITSBs supporting support brigades will interface directly with Tier 2 separate enclaves in the FRHN. ESBs/ITSBs supporting theater-level missions will interface directly with a DOD Teleport. The Army CIO/G-6 identified Army Teleport Generation II requirements in an 11 AUG 06 White Paper titled: "*Army's Adjusted Teleport Generation II Satellite Communications (SATCOM) Circuit-Switched and Internet Protocol (IP) Requirements*." For a major combat operation, teleports must be capable of supporting Tier 2 routing for seven ESBs/ITSBs and be the master reference terminal/NCC for the ESB/ITSB networks. Procedures outlined in the "*DISA Global Contingency and Exercise Planning Guide*," dated 01-2003, are required to acquire services from a teleport.

MULTIPLEXING AND LEGACY CONNECTIVITY SERVICES

I-39. The FRHN Communications Facility will house traditional devices such as fiber optic modems, copper modems, multiplexing equipment, and patch and test equipment. Inside the FRHN, the Communications Facility personnel will have the responsibility for operation and maintenance support of that equipment IAW FRHN BOIP. The theater MRHN team and division signal company will provide operation and maintenance support IAW the BOIP for the equipment at the MRHN and THN, respectively.

I-40. Promina multiplexers located at the FRHN, MRHN, and THN will be configured and managed by the Communications Facility, MRHN Team, and signal company personnel IAW BOIP, respectively. Promina multiplexers within the FRHN will be placed at the Tier 2 level and operated by the Communications Facility. Deployed force liaisons will work with Communications Facility personnel to ensure Promina configurations support end-to-end operation. The Promina multiplexers may be placed within a separate tactical domain, as required.

I-41. A General Dynamics Vantage gateway switch is present in the MRHN and THN only. The Vantage provides a secure VOIP interface into the tactical legacy voice network. The Vantage switch in the MRHN and THN will be operated by the theater MRHN team and division signal company, respectively, IAW BOIP.

ENCRYPTION SERVICES

I-42. Both bulk (e.g., KIV-19A and KIV-7HSB) and packet (e.g., KG-175) encryption devices will be located in the hub nodes. On-site operation and maintenance, configuration, and management will be provided by the Communications Facility at the FRHN, theater MRHN team, and division THN IAW the BOIP.

PRIVATE BRANCH EXCHANGE SERVICES

I-43. The private branch exchange is used to extend DSN connectivity to tactical users. The private branch exchange provides synchronous serial trunk connectivity via the Promina multiplexers to other hub nodes and JNN terminals via FDMA satellite links. These circuit switched trunks can support secure calls via secure telephone unit III and secure terminal equipment. The private branch exchange also interfaces with the Unclassified IP network, enabling VOIP users to tie into the DSN for unsecured calls. The Communications Facility personnel will provide the operation and maintenance, configuration, and management for the private branch exchange in the FRHN, while the theater MRHN team and division network support companies will operate, maintain, configure, and manage the MRHN and THN private branch exchanges, respectively. In addition, there is a requirement to include Public Switched Telephone Network access to the FRHN.

TIER 1 ROUTING SERVICES

I-44. For the purposes of this document, Tier 0 devices are DISA owned and operated, and they form the backbone and edge of the DISN network. Tier 1 devices are theater assets owned and operated by the services and CCDRs. Tier 1 devices directly connect to Tier 0 devices and extend communications into theater level enclaves. Further distinction is made in this document to Tier 1/1 and Tier 1/2 devices. Tier 1/1 devices reside at and above a theater IA boundary and interface directly to Tier 0 devices. Tier 1/2 devices reside below a theater IA boundary and interface to Tier 2 enclaves and devices. Tier 2 devices provide communications for the deployable force (tactical units).

I-45. Tier 1 NIPRNET and SIPRNET routers are installed inside the MRHN and THN. The Tier 1 routers interface with the DISA Tier 0 routers for NIPRNET and SIPRNET connectivity. They also tie into Tier 2 routers to extend packet services to the tactical users. At the FRHN, Tier 1/2 NIPRNET and SIPRNET routers will tie into existing Army Tier 1/1 routers for NIPRNET and SIPRNET connectivity. The Tier 1/2 routers inside the FRHN will be operated and maintained by the Communications Facility personnel, and configured and managed by the TNOSC. Tier 1 routers in the MRHN and THN, which are connected directly into a Tier 1 Army Theater infrastructure, will be operated and maintained by the MRHN team and division signal company, and configured and managed by the TNOSC.

TIER 2 ROUTING SERVICES

I-46. Tier 2 NIPRNET and SIPRNET routers are installed inside each hub node. The Tier 2 routers are associated with a division level routed network, but could also belong to a corps, functional area, joint operational command, or ESB/ITSB. Separate routers will be used to provide a unique Tier 2 interface within the FRHN for each supported unit's autonomous system. The operation and maintenance responsibility for the Tier 2 routers in the FRHN, MRHN, and THN is the responsibility of the Communications Facility personnel, theater MRHN team, and division signal company, respectively. The configuration and management of the Tier 2 router in the FRHN, MRHN, and THN is the responsibility of the tactical unit which controls the Tier 2 autonomous system. At a minimum, the local TNOSC will have read-only access to the full configuration and operational status of all FRHN, MRHN, and THN routers.

I-47. Figure I-3 illustrates conceptually the architecture of the Tier 2 router network at the FRHN Communications Facility, and how this architecture connects to the Tier 1, IA, and FRHN Service Facility devices.

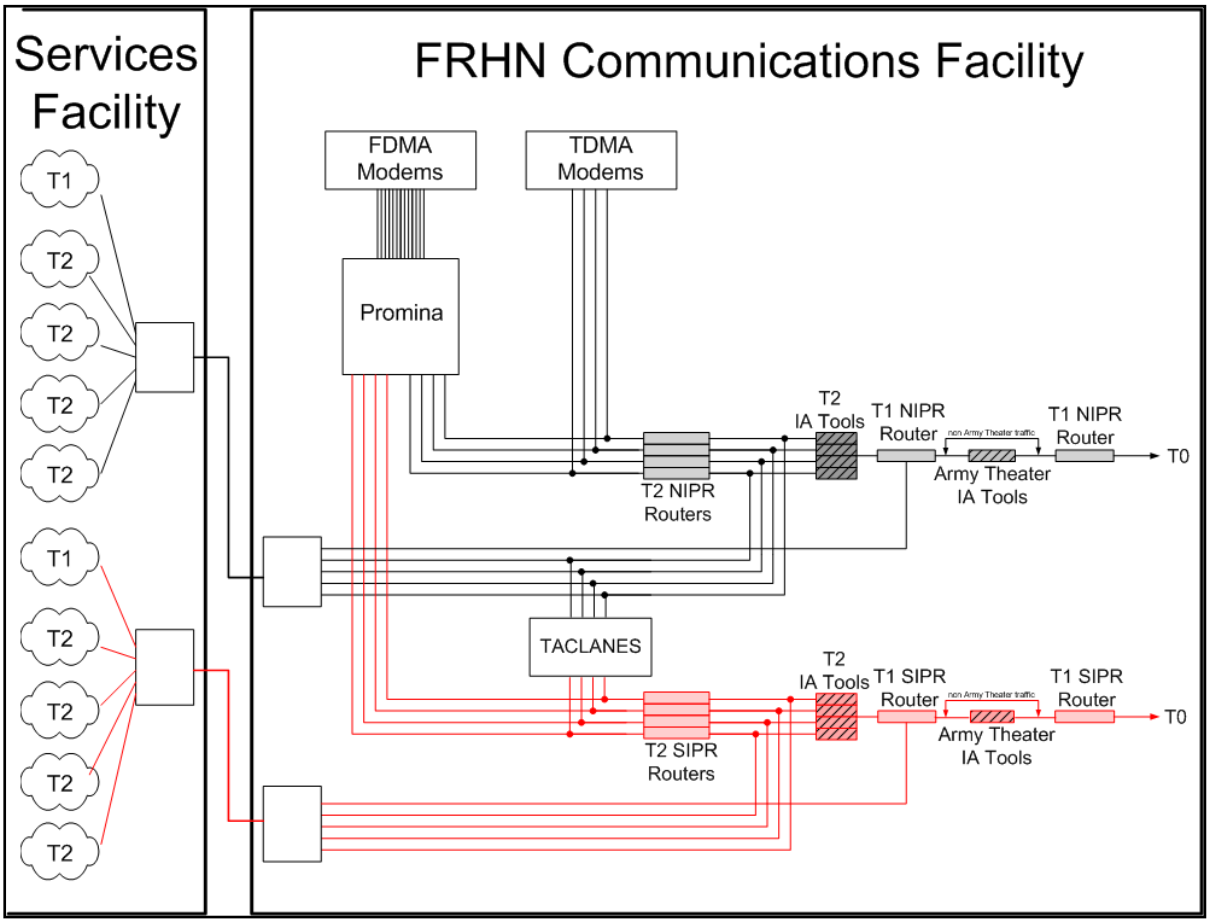

Figure I-3. Tier 1 and Tier 2 router connectivity

SECURITY SERVICES

I-48. IA border security will be installed in each hub node between Tier 1 and Tier 2 routing domains on the NIPRNET and SIPRNET connections. This border security will tentatively consist of a firewall, NIDS, and deep packet inspection device. Inside the FRHN, IA (physical or logical) will be provided for each unit supported. An additional Army theater IA stack (i.e., LWN perimeter security) will be present, or leveraged if co-located, to maintain a baseline IA boundary between Army theater users and the theater Tier 0 infrastructure.

I-49. The devices will be physically maintained by the FRHN operators, while the configuration and management will be distributed between the TNOSC and the tactical units supported. Each supported tactical unit (i.e., division or corps) will be allocated a separate physical or logical firewall instantiation to allow the unit to maintain its IA boundary and to provide a sufficient level of granularity to allow for unit-specific requirements. The supported tactical unit is responsible for the configuration and management of IA/CND equipment within the Tier 2 sanctuary created by the firewall. The tactical unit designated approving authority is responsible for ensuring all Tier 2 systems that interface with the FRHN are properly patched and meet all IA compliance criteria. The TNOSC will operate, maintain, configure, and manage the Army Theater IA stack.

I-50. Within the MRHN, the theater strategic signal brigade will operate and maintain the Tier 1 and Tier 2 IA devices, with shared management of the Tier 2 IA posture by the supported tactical unit(s). The division signal company will have operation and maintenance responsibility for the IA devices installed in

the THN. The TNOSC will provide technical oversight for all IA devices within the Army theater. At a minimum, the TNOSC will have read-only access to the full configuration and operational status of all Tier 2 IA devices within the JNN-N hub nodes. Table I-1 is a summary of the operation and maintenance responsibilities for the FRHN, MRHN, and THN services. Table I-2 identifies the configuration and management responsibilities for equipment in the FRHN, MRHN, and THN.

Table I-1. Operation and maintenance responsibilities for JNN-N hub node services

Service	*Operations and Maintenance (O&M) at FRHN*	*O&M at MRHN*	*O&M at THN*
Satellite Terminals	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Master Reference Terminal	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Multiplexers	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Private Branch Exchange	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Tier 1 Routers	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Tier 2 Routers	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Tier 1 IA Devices	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Tier 2 IA Devices	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Satellite Terminals	Communications Facility Personnel	Theater MRHN Team	Division Signal Company

Table I-2. Configuration and management responsibilities for JNN-N hub node equipment

Service	*FRHN*	*MRHN*	*THN*
Master Reference Terminal	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Multiplexers	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Private branch exchange	Communications Facility Personnel	Theater MRHN Team	Division Signal Company
Tier 1 Routers	TNOSC	TNOSC	TNOSC
Tier 2 Routers	Supported Unit	Supported Unit	Division Signal Company
Tier 1 IA Devices	TNOSC	TNOSC	N/A
Tier 2 IA Devices	Supported Unit and/or TNOSC	Supported Unit and/or TNOSC	Division Signal Company

DISTRIBUTED USER SERVICES

I-51. User services are those services that are utilized by all tactical Soldiers, regardless of branch or unit. Distributed user services are services which are implemented using a distributed server hierarchy which includes server operation and management within the tactical unit echelons. The THN and MRHN will host limited user services to support their directly connected tactical users. The FRHN will host servers to support the following functions:

- Direct support to Army theater tactical users that do not derive services from an organic or assigned tactical unit.
- Integrate and provide common user services that are also hosted at lower echelons, but require theater level support to operate across the entire AOR and between theaters.
- Provide COOP for common user services which are hosted at lower echelons within the deployed force.

I-52. The FRHN will be capable of hosting two classifications (i.e., UNCLASSIFIED and SECRET) of servers. Services above the SECRET classification level will be provided by the appropriate functional area, and are not anticipated within the JNN-N hub nodes.

I-53. Within the FRHN, Services Facility personnel (IAW the BOIP) will centrally operate and maintain the servers supporting theater-level common user services (to be determined), while deployed force liaisons will configure and manage any servers supporting their tactical users. For example, a division may pre-stage user services out of the FRHN prior to deployment, enabling subordinate units to deploy in phases and draw services from the FRHN until the division assets are completely deployed and operational. The same construct can also be used for redeployment. COOP is also a requirement, particularly for units participating in major combat operations. The FRHN will provide a stable, sanctuary location where services can be provided with a lower risk of service disruption. The following are examples of distributed common user services that could be hosted out of the FRHN. Note the initial operational capability (IOC) of the first FRHN will only include VOIP call management. When available, these services would be hosted out of an APC—

- E-mail.
- Organizational messaging.
- Domain and directory services.
- Collaboration servers.
- Information portal servers (Web servers).
- VOIP call management.
- FTP/Trivial FTP servers.
- Storage.

I-54. At the FRHN, the servers associated with these services will be located in the Services Facility. Ideally, the MRHN and THN would simply be used as a transport mechanism to reach unit services staged at the FRHN Services Facility via terrestrial connections. In certain operational scenarios, however, network connectivity between the mobile and fixed hub nodes may not support reaching back to the FRHN for certain critical user services. Therefore, at the MRHN and THN, the tactical unit may stage common user services within the baseband shelter or via transit cases as necessary.

CENTRALLY HOSTED USER SERVICES

I-55. Centrally hosted user services are those services that are currently hosted at the Army theater, joint theater, or global level, and are not actively managed by the tactical echelons. The tactical users rely on the service, and may remotely access the service to execute unit functions, but do not actively manage the service within the operational environment.

I-56. The identification of distributed versus centrally hosted user services is based upon the current architecture and standard operating procedures of each specific service. Therefore, many services which are

currently implemented using a distributed architecture may eventually become centrally hosted as more sophisticated service architectures and tactical network infrastructures are developed. This difference should be largely, if not entirely, transparent to the end user. This document lists examples of systems which are currently centrally hosted, with the understanding that this may change.

I-57. Table I-3 identifies some examples of centrally hosted user services; the organization responsible for providing the operation, maintenance, configuration, and management; and the location from where the service is provided.

Table I-3. Centrally hosted user services

Service	*O&M, configuration and management responsibilities*	*Physical location*
AKO-F	AKO Program Management Office	FRHN Service Facility APC
DNS	TNOSC	TNOSC
Anti-Virus Server	FRHN (with TNOSC configuration and management oversight)	FRHN Service Facility

FUNCTIONAL AREA SERVICES

I-58. Functional area services (sometimes referred to as Battlefield Functional Area services) are those specific battlefield operating systems that the Solders use to accomplish their mission. Examples are ABCS applications, sustainment systems, and Military Intelligence systems. These servers can be located at the FRHN or APC and configured and managed by tactical unit liaison personnel at the JNN-N hub nodes to ensure stable and single hop access to functional area AOR services.

I-59. When the unit prepares to deploy, functional area services can be pre-positioned at the FRHN Services Facility. These services can then be duplicated or moved to the THN as the operation progresses. G-6/S-6 coordination at appropriate echelons will be required to ensure assets (e.g., rack space) are reserved at the JNN-N hub nodes to support these services. In instances where the hardware and software is provided by the deployed unit, both operation and management and configuration and management responsibility will fall to the deployed force personnel requiring the service. In instances where the hardware is provided by the FRHN, the operation and maintenance responsibility for the hardware will fall to FRHN personnel while the configuration and management responsibility for the software will fall to the deployed force personnel.

NETOPS MANAGEMENT SERVICES

I-60. NETOPS management services are those services required to keep network transport systems and network devices operating efficiently and with sufficient quality of service to ensure the Soldier can achieve and maintain command and control and information dominance. Specific services are described in the following sub-sections, followed by the organization that will provide the service. The A-GNOSC is the program of record focal point to the PEOs for any NETOPS design and fielding.

I-61. It should be noted that only NIPRNET and SIPRNET NETOPS management services are provided at the JNN-N hub nodes. Coalition management services may also be hosted within a JNN-N hub node as the mission dictates. Management for TS/SCI or other higher network classification levels is not supported at the JNN-N hub nodes. TS/SCI NETOPS management services are provided at the TNCC.

Frequency Assignment Management

I-62. The SC(T) has the overall responsibility for coordinating the satellite frequency requirements for the TDMA and FDMA networks of the Army Theater. Tactical unit G-6/S-6 requiring the use of an FRHN or theater-controlled MRHN will coordinate frequency requirements with the SC(T). The SC(T) will then coordinate with the GCC J-6 (or JTF J-6) and regional DISA RSSC to lease the appropriate commercial Ku-band space segment. The Communications Facility personnel in the FRHN will coordinate closely with tactical organizations and the SC(T) to ensure spectrum allocations for the JNN-N are accurately captured

in the Spectrum XXI spectrum management system, and will be responsible for monitoring and reporting any discrepancies or issues with the JNN-N TDMA and FDMA frequency assignments.

I-63. The Communications Facility personnel operating the FRHN will conduct real-time frequency monitoring of the commercial TDMA and FDMA space segment using an L-band spectrum analyzer inside the Communications Facility. It is anticipated that a minimum of three analyzers will be available inside the FRHN for personnel to monitor active carriers on the satellites. Communications Facility personnel will coordinate with the commercial satellite service provider and tactical users to resolve frequency issues (e.g., polarization and power level adjustments, etc.). The SC(T) will coordinate with the GCC J-6 and RSSC to obtain the JNN-N transmission plan for the theater.

I-64. In the future, military Ka-band space segment will be used to support the JNN-N. When that occurs, applicable DOD spectrum management policies and procedures will be used for all Ka-band satellite links.

Time Division Multiple Access Management

I-65. The FRHN will be a participant in all TDMA meshes operating in the theater, assuming sufficient satellite and baseband resources are available. A master reference terminal and NCC combination will be established in the FRHN for all TDMA domains. A functioning master reference terminal/NCC performs overall management and control of a TDMA network, and is required for operation of the network. The master reference terminal/NCC communicates with the TDMA modems in the network and coordinates the transmissions from each terminal. Each master reference terminal/NCC will be a primary or alternate system for the TDMA domain, depending upon whether the FRHN is the controlling authority for the domain. The FRHN will be the controlling authority for the TDMA domains supporting theater level JNN-N users and functional area users supported by JNN-N assets. The FRHN will also be the controlling authority for JNN-N units that are transiting into or out of the theater. At the FRHN, the master reference terminal/NCC platforms will be installed in the Communications Facility and configured and managed by the Communications Facility satellite support personnel.

I-66. The FRHN would also be the controlling authority for a BCT deployment in an expeditionary mode. In this scenario, the FRHN would provide both the primary and alternate master reference terminal/NCCs.

I-67. When a THN is deployed and operational in a theater, the THN is the controlling authority for the TDMA domains supporting its subordinate units. The THN would have the primary master reference terminal/NCC responsibility, and the FRHN would provide the alternate master reference terminal/NCC capability.

Frequency Division Multiple Access Management

I-68. The FDMA links are single channel per carrier links. In the JNN-N equipped units, these are all currently setup for Ku-band transmission (Ka-band supported in the future). While the same satellite modem is used throughout the JNN-N to ensure interoperability, the modem is generally compatible with other FDMA single channel per carrier satellite modems and will communicate with a variety of military multi-band terminals and DISA Teleport facilities via Ku-band transmission. Detailed monitor and control of the satellite modems is performed via the front panel interface. A monitor and control capability for the satellite modems and other equipment in the radio frequency and intermediate frequency chain is also performed using a monitor and control application. At the FRHN, the monitor and control application will be installed inside the Communications Facility and will be operated and maintained by the Communications Facility satellite support personnel.

I-69. The controlling authority for each FDMA link will be the higher echelon organization. For example, the FRHN would be the controlling authority for an FDMA link between the FRHN and a JNN at the BCT. If a BCT has an FDMA link into a JTF headquarters, then the JTF would be the controlling authority for the circuit.

Network Monitoring and Management

I-70. One of the near-term challenges is the expectation that the network management applications used in the TNOSC are different than the management applications used in the JNN-N. In the near-term, one or more network management tools may be required at the FRHN Services Facility to allow tactical network management data to be hierarchically consolidated at the Army theater level. The network monitoring tools at the FRHN and MRHN will also be able to act as an alternate network monitoring capability for the tactical unit if the tactical unit-owned network monitoring platform is temporarily out of service. The Tier 1 FRHN monitoring platforms will be operated, maintained, configured, and managed by the Services Facility personnel.

I-71. Tier 2 FRHN monitoring platforms will be operated and maintained by Services Facility personnel, and configured and managed by liaison personnel from the supported tactical units. JNN-N network management data will be integrated into the TNOSC for network common relevant operational picture purposes and forwarded to the A-GNOSC. As NETOPS management applications are standardized across the Army, theater NETOPS servers will be consolidated at the TNOSC. The TNOSC is also capable of providing network common relevant operational picture views to joint NOSCs when supported units are operating in a joint environment.

I-72. The MRHN will also have the standard tactical network management suite of applications and hierarchically report its information to the FRHN, if present, or alternatively to the TNOSC. Likewise, the THN has the standard tactical application suite and reports its information vertically to an FRHN or MRHN, as appropriate.

I-73. The tactical unit has management and configuration control of network monitoring within its AOR. Therefore, the hierarchical view provided to the FRHN shall be read-only, allowing the FRHN and TNOSC personnel to determine network status. The FRHN will have read/write access for theater level (i.e., Tier 1) assets. There are ongoing efforts to integrate the deployable force and theater network management and trouble ticketing systems to provide a near real-time status and hierarchical reporting of the JNN-N status.

Firewall Management Server

I-74. Host LAN and perimeter firewalls are installed throughout the JNN-N on NIPRNET and SIPRNET connections. Multiple firewalls (physical or virtual) will also be located within the THN, MRHN, and FRHN, depending on the number of different autonomous routing domains (i.e., different divisions, expeditionary brigades, or functional area units) supported. Firewall management platforms will be installed in each of the hub nodes. The BCTs also have an organic firewall management capability for use during autonomous operations.

I-75. The firewall manager will be operated and maintained by the Services Facility at the FRHN, and by the Theater MRHN Team and division signal company at the MRHN and THN, respectively. At the FRHN, the firewall management server will reside in the FRHN Services Facility. Each supported tactical unit will have the responsibility of properly configuring the Tier 2 firewalls within their unit AOR per the technical direction from the TNOSC and RCERT. The supported tactical units will be able to leverage the FRHN, MRHN, and/or THN firewall management server to manage firewalls within their unique AORs.

Tactical Local Area Network Encryptor Management

I-76. The General Dynamics Tactical FASTLANE Tactical Local Area Network Encryptor (TACLANE) (KG-175) is a National Security Agency certified Type 1 packet encryption device used in the JNN-N architecture to tunnel classified traffic across the BLACK core network. The General Dynamics ESM/NM Encryptor Manager Solo version is installed in each of the hub nodes. The NM/ESM Encryptor Manager Solo in the THN is currently used to manage all of the TACLANEs in the division JNN-N infrastructure. The NM/ESM Encryptor Manager Solo in the FRHN and MRHN will manage and configure their Tier 1 TACLANEs. Any Tier 2 TACLANEs will be configured and managed by the deployed force unit.

I-77. At the FRHN, the ESM/NM Solo will be installed in the FRHN Services Facility and will be operated, maintained, configured, and managed by Services Facility personnel. The NM/ESM Solo in the MRHN and THN will be operated, maintained, configured, and managed by the network administrators operating in the baseband shelter.

I-78. The BCTs also have the Lite version of the ESM/NM Encryptor Manager Solo application for use during autonomous operations.

I-79. It should be noted that the TACLANE device can only be monitored and managed by a single ESM/NM. Consequently, it is imperative that clearly delineated roles and responsibilities are established and maintained.

Router and Switch Management

I-80. Router and switch element management capabilities exist in each of the hub nodes, as well as the JNNs at brigade, division, and corps levels. The responsibility for router and switch operation and maintenance is the same as depicted in Table 8-1 above. The responsibility for Tier 1/2 router and switch configuration and management within the FRHN, MRHN, and THN is the same as depicted in Table I-2 above.

I-81. The element management capability at the THN and JNN will be used to manage and configure the Tier 2 routers and switches within the division and BCT, respectively. The element managers at the MRHN and FRHN will be used to manage and configure routers and switches that are theater level assets and any functional area users supported directly from either of the hub nodes. The element managers at the MRHN and FRHN can also be leveraged by the supported unit to manage and configure Tier 2 devices within the unit AOR.

Network Equipment Technologies Inc. Promina Element Management

I-82. A Promina element manager will be installed in the FRHN Communications Facility. The element manager will have the capability to manage, monitor, and configure all JNN-N Promina resources in the theater. Inside the FRHN, the Communications Facility personnel will operate, maintain, configure, and manage the element management platform. For theater level operations, the SC(T) will develop and coordinate the overall JNN-N multiplexer plan with the GCC J-6 and DISA field offices, where appropriate. The multiplexer plan will be distributed to theater and division G-6/S-6 representatives for implementation.

I-83. Each hub node and JNN will configure, operate, and maintain their respective Promina multiplexers, while permitting visibility into their Promina via the element manager located at the FRHN. Excluding the FRHN, units will monitor and configure their Promina multiplexers using the console interface.

Network Intrusion Detection System Management Services

I-84. The JNN-N NIDS architecture consists of NIDS sensor devices which collect and forward network information to a NIDS management platform. NIDS sensor devices are installed in all of the JNN-N hub nodes between the Tier 1 and Tier 2 routers, as part of the IA stack. NIDS sensor devices are also installed throughout the JNN-N network. Two NIDS event correlation and management platforms (such as, UNCLASSIFIED and SECRET) will be installed in each FRHN, MRHN, and THN. In the future (time to be determined), network IPS devices are planned to replace NIDS devices in the Army's IA architecture.

I-85. The FRHN Services Facility, Theater MRHN Team, and division signal company will operate and maintain their respective NIDS management platforms and NIDS sensors within the FRHN, MRHN, and THN. All Tier 1 NIDS in the FRHN, MRHN, and THN will be configured and managed by the TNOSC. Tier 2 NIDS in the FRHN, MRHN, and THN will be configured and managed by tactical unit liaisons, Theater MRHN Team, and division signal company, respectively. JNN-N units can choose to send NIDS sensor data directly to the NIDS management platform within the FRHN or to the NIDS management platform within the THN (when available).

I-86. Regardless of which hub node is used to collect sensor data, tactical units may access the corresponding NIDS management platform to view and manage NIDS events within their AOR. Event and log data from all hub NIDS management platforms will be forwarded to the TNOSC for analysis. Signature policies will be set by the A-GNOSC and promulgated via the TNOSCs to the respective units.

Network Common Relevant Operational Picture

I-87. The FRHN Services Facility is responsible for consolidating all Army NETOPS data from the tactical environment in support of theater operational commands. The TNOSC will be responsible for integrating relevant data from the tactical environment to build the theater network common relevant operational picture. The TNOSCs will further forward network common relevant operational picture data to the A-GNOSC for global Army NETOPS SA. Upon request, the TNOSC will provide remote access views into the theater network common relevant operational picture for the tactical user's SA.

Vulnerability Management Services

I-88. Vulnerability assessment and remediation servers (e.g., Hercules and Retina) will be installed at the UNCLASSIFIED and SECRET levels in each of the JNN-N hub nodes. The operation and maintenance of vulnerability management servers will be performed by Services Facility personnel, theater MRHN Team, and division signal company for their respective hub nodes. The FRHN, MRHN, and THN vulnerability management servers will be configured and managed by the TNOSC, theater, MRHN Team, and division signal company, respectively. Supported tactical units will conduct local vulnerability management for devices with unit-controlled sanctuaries located at the FRHN Services Facility. Similarly, the theater MRHN Team and division G-6 personnel will provide vulnerability management support for the MRHN and THN, respectively. The TNOSC will provide technical guidance.

Service Desk

I-89. A distributed trouble ticket application is expected to be used throughout the JNN-N, and is typically operated by the TNOSC and supported units S-6/G-6. This hierarchical service desk capability extends through the division and/or corps level to the theater and global Army levels. When a separate joint chain of command exists within the joint operational area, trouble ticket information is also exchanged with the joint command.

I-90. One of the near-term challenges is the trouble ticket application used in the TNOSCs are different than the application selected for use in the JNN-N. The lack of integration among disparate applications results in manual intervention to maintain trouble tickets and work flow across application boundaries. In the near-term, service desk tools compatible with those fielded throughout the JNN-N will be required at the FRHN Services Facility to allow incidents, problems, and changes being tracked within the JNN-N to be hierarchically consolidated at the theater level. This will allow FRHN personnel visibility of the incidents, problems, and changes being tracked within the JNN-N service desk tool. These tools will be operated and maintained by the Services Facility personnel. Future efforts will address the integration of service desk tools used in the JNN-N architecture and at the TNOSCs for network common relevant operational picture and global workflow purposes.

I-91. In the interim, the FRHN will have a limited service desk capability to maintain visibility into JNN-N incidents, problems, and changes as described above. This will allow tactical users to escalate trouble tickets for theater level issues to the FRHN electronically. This will allow the TNOSC to track critical incidents, problems, and changes in its Service Desk application while prioritizing FRHN work based on theater mission requirements. It should be noted that there will be no automated synchronization between the JNN-N and TNOSC Service Desk applications. The FRHN will operate using a pre-established criteria published in an OPORD published by the A-GNOSC for the reporting of incident, problem, status, and change information to the TNOSC and A-GNOSC.

I-92. Trouble tickets for TS/SCI users will still be the responsibility of the TNCC Network Management Help Desk staff. Trouble tickets will be coordinated with the Services Facility service desk staff as needed. This collaboration must be worked out as part of the JNN testing of TS/SCI requirements.

FIXED REGIONAL HUB NODE OPERATIONS AND CONTROL PLAN

BACKGROUND

I-93. The introduction of the AN/FSC-133 FRHN will enable the deployment of JNN-N equipped or compatible units into a theater where they can immediately begin to draw their satellite and Defense Information Systems Network (DISN) services from a fully pre-positioned hub node operating in sanctuary. The FRHN NOC will activate satellite carriers prior to the flow of forces into the theater as well as DISN connectivity for deployed force access to national networks. The FRHN is the primary hub node when a THN is not present in-theater. Additionally, it provides backup services in support of a division when their THN is deployed and fully operational and will be the primary hub node for ESBs supporting corps or theater Army assets. The FRHN can also provide service to other service components (e.g., Air Force and Marines), provided their terminals are compatible with the SATCOM and baseband equipment inside the FRHN. The procedures outlined in this document would also be used by the other service components.

PURPOSE

I-94. The purpose of the FRHN Operations and Control Plan is to establish an integrated framework with standardized terminology and to consolidate operations, management and control policies; processes; and procedures for the FRHN NOC and JNN-N enabled/compatible units. This manual identifies the processes that will be utilized to allocate and manage services provided by the FRHN. It also outlines how some existing processes will be modified to meet the specific needs of the FRHN and how services are provided by the FRHN. One of the primary objectives is operational agility, which will allow services to be provisioned quickly upon initial entry. Of equal importance is the placement of mechanisms to facilitate rapid change to meet the Soldier's evolving requirements during all phases of full spectrum operations. Figure I-4 illustrates where the FRHN fits in an overall communications hierarchy. To achieve a high degree of operational agility, the following capabilities will need to be realized:

- Well defined DAA chain and a streamlined authority to connect (ATC)/ATO process IAW the DOD Information Assurance Certification and Accreditation Process (DIACAP) dated 28 November 2007.
- Pre-positioned or pre-negotiated SATCOM space segment.
- Pre-positioned baseband services and the use of connectivity templates.

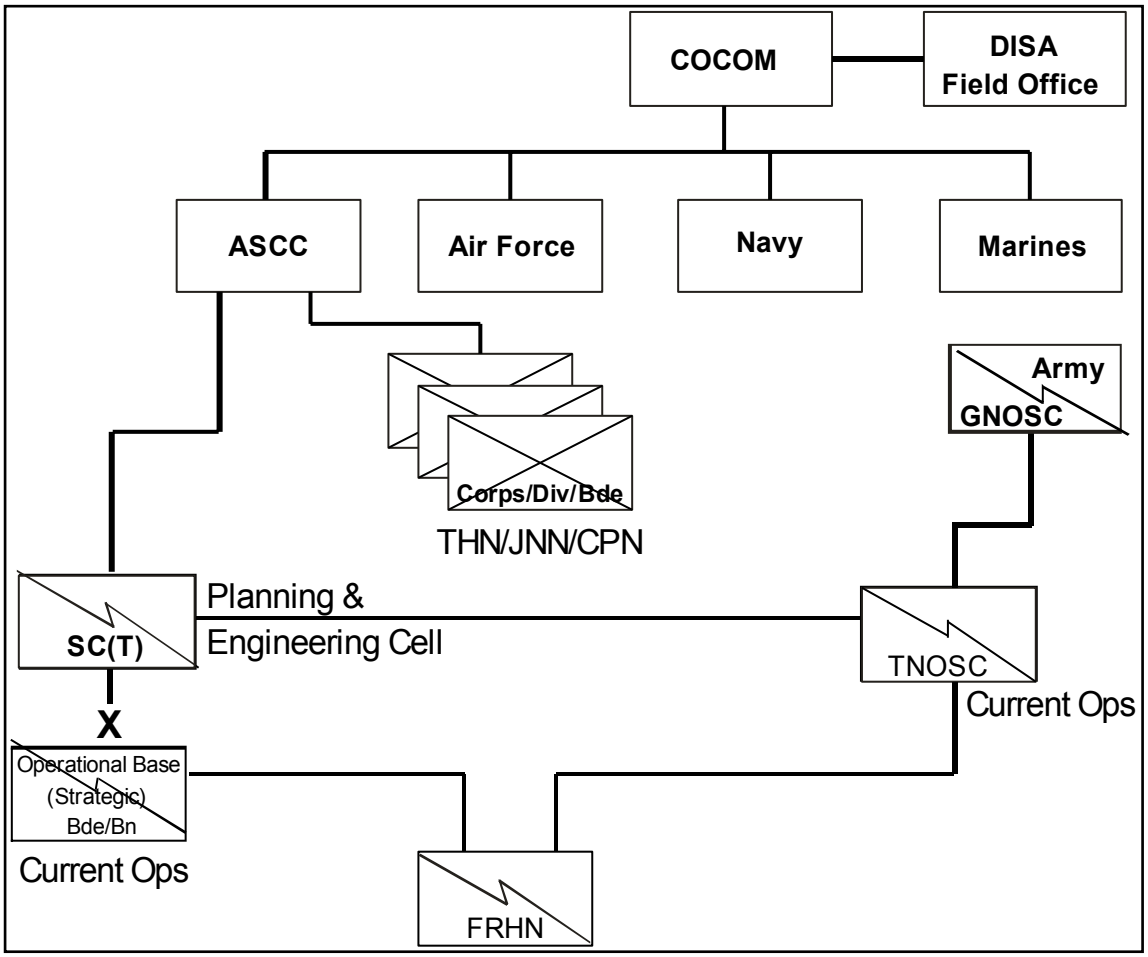

Figure I-4. FRHN hierarchical relationship

FRHN CAPABILITIES

I-95. This section describes the services that the FRHN will be capable of providing to the JNN-N enabled/compatible unit to include cross-service support, e.g. the US Marine Corps). The services provided to the JNN-N enabled/compatible units fall into two categories: wideband access services and baseband access services.

WIDEBAND (SATELLITE) ACCESS SERVICES

I-96. The FRHN can provide access, via TDMA and FDMA satellite, to DISN services for up to three divisions (or two divisions and four separates (e.g., expeditionary BCT, ESB, etc.). The FRHN is fielded with 48 FDMA modems, 48 TDMA modems, and 16 mounted battle command on the move modems. Rack space is also being reserved for potential integration of Army Airborne Command and Control System integration into the FRHN.

I-97. The goal is to have a set amount of pre-provisioned space segment available in each AOR to support short notice warfighter deployments. The pre-provisioned space segment would be supplemented with a process to rapidly procure additional space segment to support the additional flow of forces into the AOR. This capability is still in the early stages of development. The capability and its associated processes/procedures will be provided in separate correspondence and upon subsequent update of this document.

I-98. The FRHN will serve as the controlling earth terminal for access to and maintenance of the satellite links between itself and the JNN-N enabled/compatible units. As the controlling earth terminal, the FRHN NOC will act as the intermediary between the JNN-N enabled/compatible units and the commercial satellite NOC. The tactical unit will contact the FRHN NOC to initiate initial access or troubleshooting. The FRHN NOC will bring up the commercial SATCOM NOC in a three-way conference call. Direction for transmit power initiation, adjustments, and polarization changes can come only from the DISN Satellite Transmission Service-Global contractor.

I-99. When the Wideband Global SATCOM constellation is operational, and JNN-N equipped/compatible units and FRHNs are capable of Ka-band operations, the operational control for the Ka-band trunks will be performed by the USSTRATCOM Wideband Satellite Operations Center.

BASEBAND (DISN) ACCESS SERVICES

I-100. The FRHN will have a permanent set of DISN subscriber services through the normal request for service/telecommunications request/telecommunications order process with DISA, and these services will be established at FRHN IOC. This set of DISN subscriber services will be extended to requesting JNN-N enabled/compatible units via a Tier 2 to Tier 1 Army Service Request (ASR) submitted to the SC(T) via the ASCC. If the requirement cannot be met by existing FRHN DISN resources, the SC(T) will coordinate with the ASCC to provision additional services via the telecommunications request/telecommunications order process. The key to the IOC DISN subscriber services provisioning process is to establish an amount of pre-positioned services such that the probability of having to provision additional services via request for service/telecommunications request/telecommunications order process is minimized to the greatest extent possible. Avoiding this time intensive process will help maintain a high degree of operational agility.

I-101. Figure I-5 provides a graphical representation of this concept. As shown, a set of DISN subscriber services from the DISN at Tier 0 (i.e., DSN and DRSN) will be pre-provisioned and activated to the FRHN at Tier 1. The FRHN will interface to an existing Tier 1 LWN perimeter security stack (co-located on the installation) for access to NIPRNET and SIPRNET. JNN-N enabled/compatible units at Tier 2 will request access to DISN services from the FRHN and access those services via the FRHN's Tier 1 connectivity, rather than directly from the DISN at Tier 0. Upon request, the FRHN NOC will allocate DISN services to the requesting JNN-N enabled unit from its pre-provisioned set of DISN subscriber services.

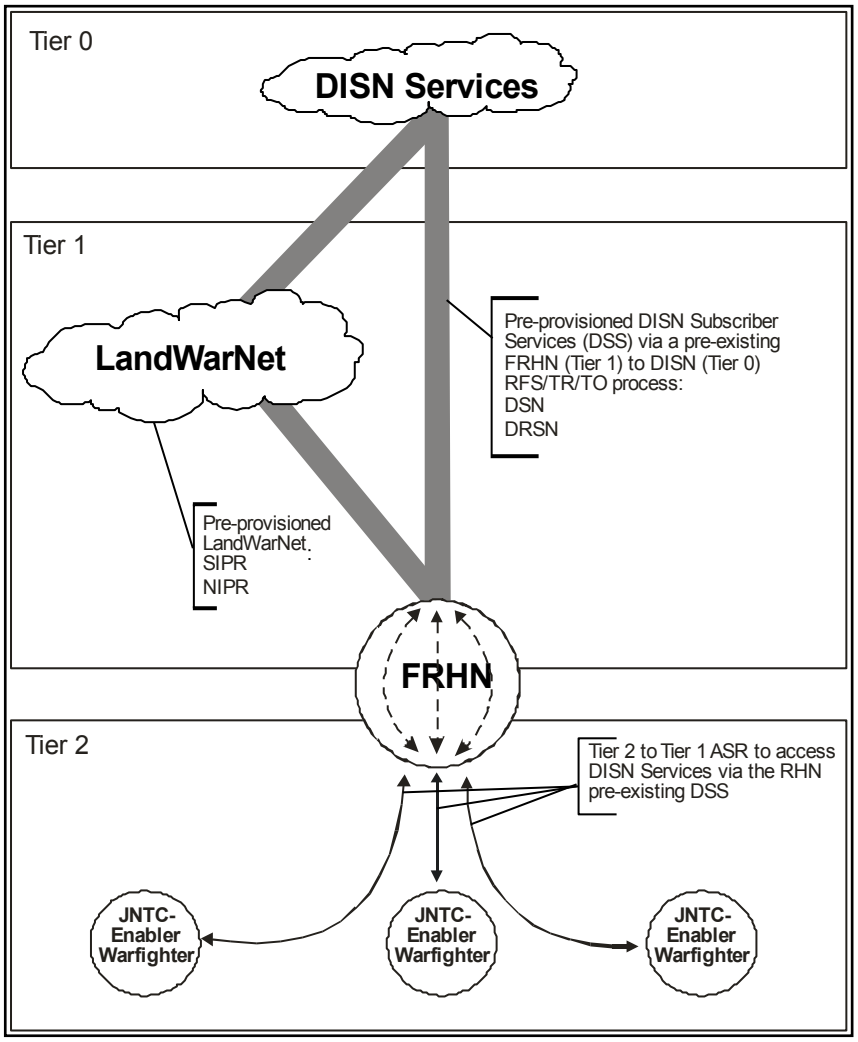

Figure I-5. FRHN/JNN-N DISN services design model

I-102. The DISN operates as a sub-element of the GIG, providing the DOD with consolidated worldwide telecommunications infrastructure that delivers the end-to-end information transfer network for support to military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. DISN provides interoperable, secure IP data communications services such as NIPRNET and SIPRNET, as well as voice communication services such as DSN and DRSN. Video teleconferencing services are also offered via DISN Video Services-II, which is a pass through service in the FRHN. Examples of services that would be provided through the FRHN are—

- **NIPRNET** provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet.
- **SIPRNET** is the DOD's largest interoperable command and control data network supporting the Global Command and Control System, the Defense Message System, collaborative planning and numerous other classified Warfighter applications.
- **DSN** provides command and control circuit switched service. As a command and control network, the DSN has military requirements to provide assured service and global connectivity under stress conditions. The switched voice service of the DSN allows calls originated from

DISN locations to be connected to any other DISN location. The service includes long-haul switched voice, facsimile, and conference calling.

- **DRSN** is the secure command and control system and is a key component of the DOD global secure voice services. The DRSN supports the secure voice and secure conferencing requirements of the President or the SECDEF or their duly deputized alternates or successors, National Command Authority, components, DOD, and select federal agencies in peacetime, crisis situations, and wartime. It is a separate, secure switched network that is considered part of the DISN. Access to this network is provided IAW CJCSI 6215.01C.
- **DISN Video Services-II**, controlled under DISA's GIG-Combat Support Branch, is responsible for management and oversight of the DISN Video Services-II implementation and program sustainment. This replacement to the DISN Video Services-Global is IP based and supports Integrated Services Digital Network users.
- **Unclassified VOIP** service is provided in the JNN-N. The FRHN has the ability to bridge the JNN-N VOIP into the DSN for worldwide voice communications.
- **Secure VOIP** is a closed VOIP system that operates on the Secret JNN-N IP network infrastructure. The system operates at the Secret-High level.

I-103. The project manager for DCATS will provide the FRHN Type Accreditation to the SC(T) DAA. The SC(T), as the DAA for the theater LWN (to include the FRHN), will issue the FRHN ATC for connection to the Army theater (Tier 1) point of presence. Additionally, the SC(T) will submit an ATO to the DISA DAA and obtain the ATC for FRHN services that connect directly to DISA Tier 0. The FRHN Type Accreditation effort will be accomplished as part of the FRHN IOC. This process is illustrated in Figure I-6.

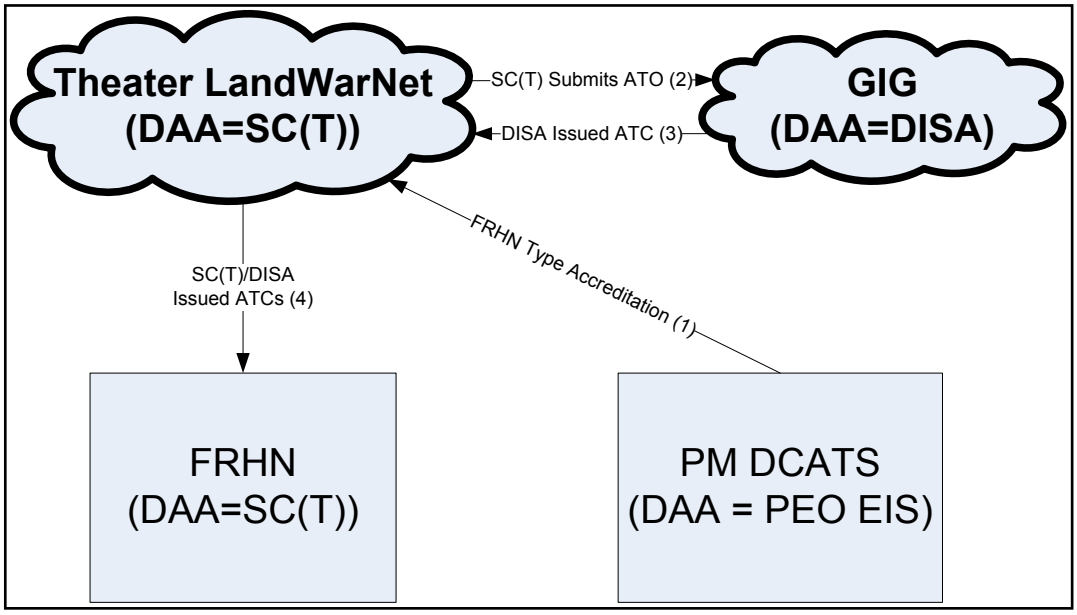

Figure I-6. ATO/ATC process for FRHN IOC

REQUESTING FRHN SERVICES

I-104. This section describes the process that will be followed to request satellite and gateway connectivity into the FRHN. These requests will leverage and utilize DISA's SAR and Gateway Access Request (GAR) procedures. It is important to note that these procedures have been streamlined for the sake of operational agility. SAR and ASR templates will be available on NETCOM/9th SC(A)'s Regional Hub Node AKO portal (AKO Files →U.S. Army Organizations →Army CIO/G-6 →NETCOM 9th SC(A) →Headquarters Staff ACofS, →G-3 Knowledge Centers Regional Hub Node) or the United States Army

Forces Command (FORSCOM) G-6 Spectrum Management AKO portal (AKO Files U.S. Army Organizations →FORSCOM Knowledge Centers →G6 →Spectrum Management). For all space segment requests, a SAR will be required. A SAR will also be required if changes are made to the existing allocation of the satellite space segment, or terminating equipment (e.g., antenna size) change. This is due to the continued need to interface with the GSSC or RSSC as an interface to the DISN Satellite Transmission System-Global for generation of a transmission plan, licensing, etc. The SC(T) will submit a request for service to DISA to establish initial DISN services provisioned to the FRHN. This will be accomplished as part of the IOC of the FRHN.

I-105. A request for service and telecommunications request will be submitted by the SC(T) to DISA if the baseband and/or DISN Tier 0 service requirements exceed the quantity pre-positioned and/or installed DISN services at the FRHN. An ASR will be submitted by the Soldier to the ASCC for the original requirement. An ASR is a modified GAR that is scoped for FRHN baseband operations. The ASR is not intended to go to DISA for any actions and will be handled internal to the theater Army organizations in a highly expedited manner.

I-106. ESBs supporting division and corps assets will obtain Ku-band (future Ka-band) services from the FRHN using the SAR/ASR process. The ESB's supported S-6/G-6 will be responsible for submitting the SAR and ASR. The ESB S-3 or SB(T) will assist the supported unit with SAR and ASR development. ESBs may support joint operations (e.g., JTF) and may derive their services via a DOD Gateway. This would require a normal DISA SAR and GAR submission. All X-band requirements (Ground Mobile Force and Phoenix terminals) for service through a DOD gateway will continue to follow the DISA SAR and GAR submission procedures. Note that the IP connectivity (e.g., NIPRNET and SIPRNET) between the FRHN and co-located gateway will be accomplished via Army Tier 1 and DISA Tier 0 connectivity on the installation therefore, terminals downlinking at a DOD gateway will have high-bandwidth, low-latency connectivity to users operating off of the FRHN. The ability to leverage a local LWN perimeter security stack will provide a high level of assured connectivity between FRHN and DOD Gateway customers by keeping the interface local to both facilities, thereby keeping traffic between them internal to the theater.

I-107. The FRHN is the intermediary between the DISN and the JNN-N enabled units, and will extend access to DISN services to the JNN-N enabled tactical unit. As part of the initial communications request, the Deployable Forces will submit an ATO to the SC(T) to obtain the required ATC. While this is part of the initial request package that is submitted to the ASCC, the SC(T), as the FRHN DAA, is responsible for issuing the ATC. This process is shown in Figure I-7.

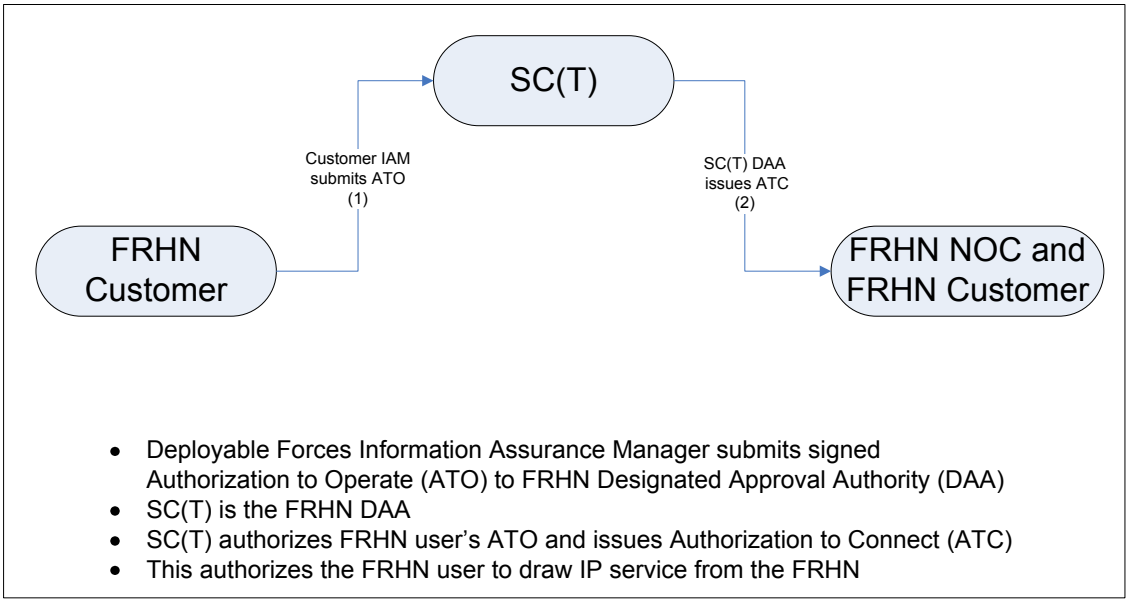

Figure I-7. ATO and ATC process for user connection to FRHN

DETAILS OF THE SATELLITE ACCESS REQUEST/ARMY SERVICE REQUEST PROCESS

I-108. Each JNN-N enabled Soldier will be required to possess an interim authority to operate (IATO) certification from their responsible DAA prior to the submission of their SAR/ASR.

I-109. Figure I-8 outlines the SAR/ASR process that will be used for training. Training missions are assumed to be conducted within Army channels; therefore the only external interaction is with DISA SATCOM entities.

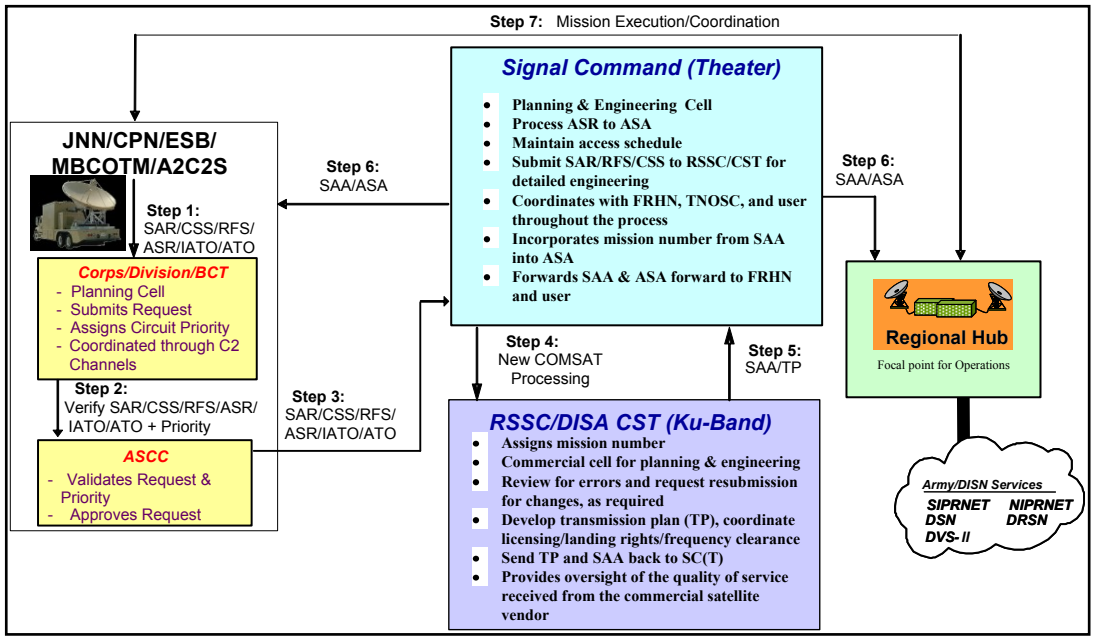

Figure I-8. SAR/ASR process for training missions

I-110. The top half of Figure I-9 illustrates the SAR/ASR process for exercises and operational missions. In this process, it is assumed that tactical units will be operating in a joint environment, and as a result there will be CCDR adjudication/validation of resource usage. The following organizational references only identify parent organization relationships. Inter-organizational communications and coordination will be handled IAW standard Army doctrine, policy, and procedures.

I-111. **Step 1**: Soldier submits a SAR, request for service, Commercial Satellite Team (CST) Service Survey, ASR, network diagram and ATO/IATO to the theater ASCC (OCONUS) or US Army Forces Command (CONUS). Other steps required are listed below:

- Warfighter coordinates with corps/division (as appropriate/applicable) during the development and submission of the SAR/request for service/CST service survey/ASR, network diagram, and ATO process.
- The corps validates the submission paperwork and forwards to ASCC/FORSCOM.

I-112. **Step 2**: ASCC/FORSCOM validates request and assigns mission priority and conducts the following:

- ASCC coordinates with the SC(T) and the FRHN NOC to ensure resources are available to support mission requirements.
- ASCC coordinates requirement with CCDR if: space segment is funded by CCDR; Joint mission supported (e.g., JTF); adjudication of resources necessary for competing joint mission requirements.
- If disapproved, the SAR/ASR is sent back to the requesting unit noting disapproval. Alternate COAs may be conducted as follows:
    - The ASCC and SC(T) will work with the tactical unit to identify alternative COAs (e.g., Out-of-theater FRHN or Teleport access).
- ASCC submits SAR/CST service survey to the organization responsible for commercial SATCOM management. The commercial SATCOM manager for CONUS is located within NETCOM/9th SC(A). The commercial SATCOM manager for OCONUS is located within the SC(T).

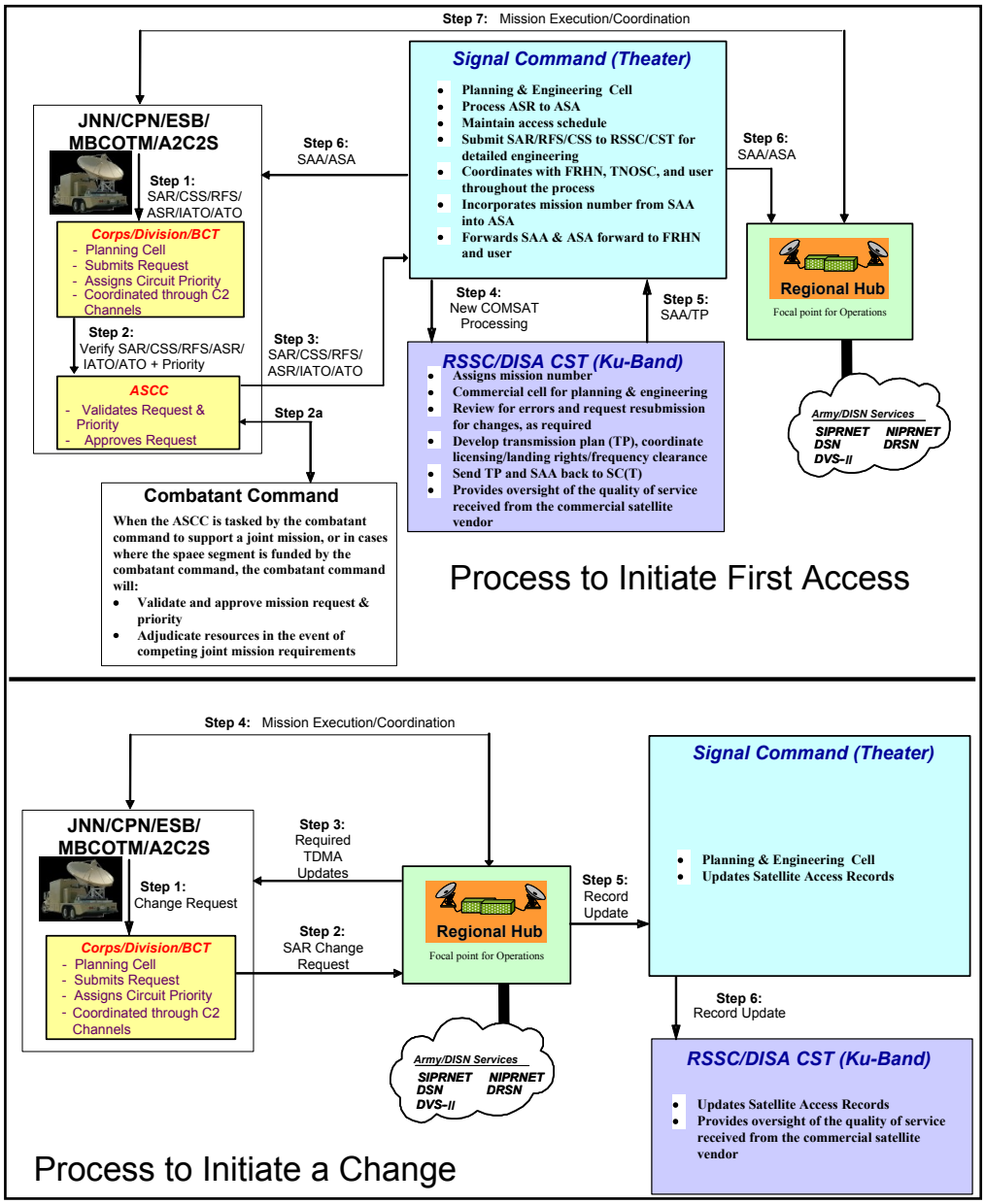

Figure I-9. SAR/ASR process for exercises and operational missions

I-113. **Step 3**: SC(T) or NETCOM/9th SC(A) incorporates mission requirement into SATCOM access schedule: Determines whether there are competing requirements for space segment resources and adjudicates conflicts with ASCC and/or CCDR for Army or Joint missions, respectively.

Step 4: SC(T)/NETCOM/9th SC(A) forwards SAR/CST service survey to the GSSC or RSSC before the following happens:

- The GSSC/RSSC satellite support center receives SAR/CST service survey from commercial SATCOM manager and submits the package to the commercial satellite vendors.
- The DISN Satellite Transmission System-Global contractor selected develops transmission plan and coordinates licensing, landing rights, and frequency clearance.
- The GSSC/RSSC assigns mission number and develops the satellite access authorization (SAA).

I-114. **Step 5**: The SAA and transmission plan are sent back to SC(T)/ NETCOM/9th SC(A). In the case of training missions, the commercial SATCOM manager tracks space segment utilization. In the case of joint missions (exercise and operational), the commercial SATCOM manager disseminates the SAA and transmission plan to the CCDR J-6 for theater space segment utilization and frequency management. The SC(T) also:

- Reviews IATO/ATO and authorizes connectivity.
- Coordinates with FRHN NOC to identify equipment set to support mission.
- Develops the Army Service Authorization (ASA) from the ASR and incorporates the mission number from the SAA into the ASA.

I-115. **Step 6**: The SC(T)/NETCOM/9th SC(A) provides the ATC, ASA, and SAA/transmission plan to the tactical unit and FRHN NOC. The FRHN and tactical unit—

- Coordinate, as necessary, the development of equipment crew assignment sheets.
- Implement crew assignment sheets and prepare systems for operation such as—
    - FRHN NOC develops crew assignment sheets and implements equipment configurations as per SAA/ASA/transmission plan/crew assignment sheets, and provides coordinating authority for satellite and baseband services at the FRHN.
    - Tactical unit implements equipment configurations as per SAA/ASA/transmission plan/crew assignment sheets and coordinates with the FRHN NOC for access to satellite and baseband services.

I-116. The bottom half of Figure I-9 illustrates the process to make a change to the original SAA once the mission has already been initiated. For changes that don't affect the space segment or power allocation on the transponder, the process can be streamlined to support the Soldier's needs. For example, if a battalion is directed to jump to another location, the associated battalion CPN would also be geographically relocated. Prior to the jump, the FRHN may need to cut a new boot file for the CPN's Linkway modem to update latitude and longitude information (or other) to ensure transmit and receive synchronization when the CPN comes up at its new location. This coordination and execution can be handled rapidly between the unit's S-6/G-6 and the FRHN NOC. The FRHN NOC would notify the SC(T) of the minor changes. The SC(T) would notify the RSSC /GSSC of the terminal location changes.

I-117. In establishing the service, the JNN-N equipped/compatible unit will work with the FRHN NOC to initiate and troubleshoot the service as required. The FRHN NOC will in turn establish the required coordination with the commercial satellite NOC.

I-118. DISN services will be extended to the JNN-N enabled/compatible tactical unit by the FRHN from a pre-positioned set of DISN subscriber services. These services include, but are not limited to, SIPRNET, NIPRNET, DSN, DRSN, and DISN Video Services-II. Since the JNN-N enabled/compatible tactical unit's gateway connectivity into the DISN will be extended and managed by the FRHN NOC, the JNN-N enabled/compatible unit will submit an ASR to the SC(T) (via the ASCC) rather than to the DISA Regional Contingency and Exercise Branch to request gateway access to DISN services. The JNN-N enabled/compatible unit's ASR will be internal to the Army, as direct connectivity to DISN services will be pre-positioned. However, in the event the FRHN NOC is unable to fulfill a mission requirement (due to competing or higher priority missions, special circuits, or user-requested STEP circuits), the deployed user will be responsible for submitting a GAR to the DISA contingency and exercise (via the CCDR for validation) to request baseband equipment and/or DISN service access via the DOD Gateway.

I-119. For extension of DISA services that the FRHN is not configured or pre-provisioned to support (e.g., Joint Worldwide Intelligence Communications System encrypted serial circuit), the unit will be required to submit a GAR via the standard DISA process. The SC(T) and FRHN NOC will assist the unit with the request to ensure the proper services are provisioned and extended via the hub node.

I-120. A FRAGO ASR is required to initiate a change request to existing FRHN baseband services provisioned to the unit. A FRAGO ASR is required for any baseband changes driven by mission

requirements. The FRAGO ASR is not intended to go to DISA for any actions and will be handled internal to the theater Army organizations in a highly expedited manner. It should be noted that not all adjustments will require theater Army adjudication, requiring only coordination with the FRHN NOC. This will further streamline the process and keep responsiveness at the necessary level. The FRAGO ASR process is highlighted in Figure I-10.

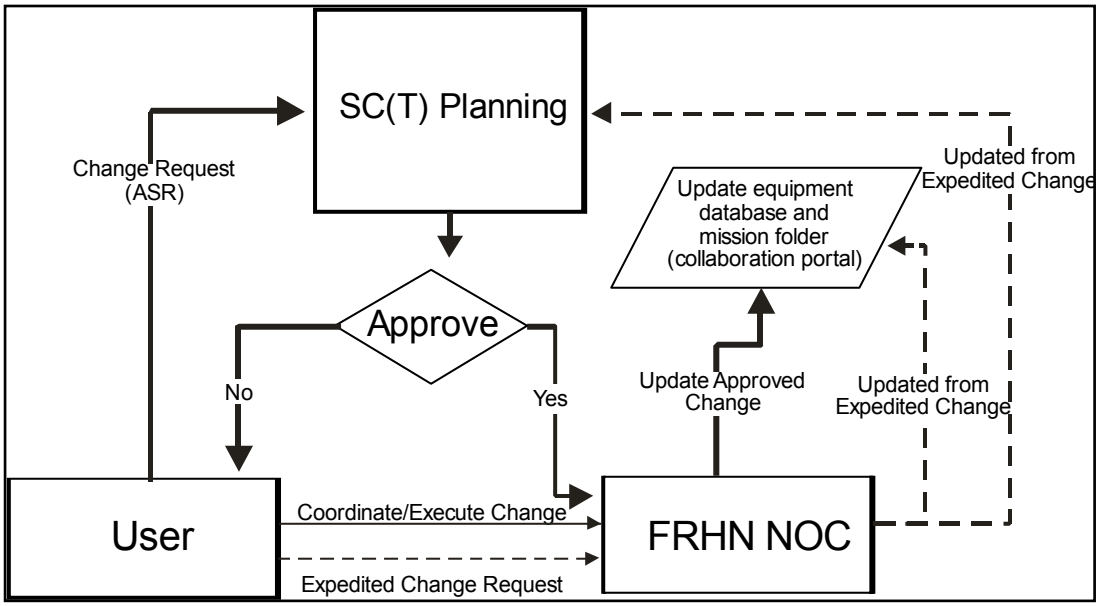

Figure I-10. Change request process

FIXED REGIONAL HUB NODE SITE ADMINISTRATION AND OPERATION

I-121. This subsection describes critical areas of operational management and site administration for the FRHN. Once the mission is validated and the unit is drawing services from the FRHN, any requests for additional services should be coordinated via an ASR with the SC(T).

FRHN DISN SERVICES PROVISIONING

I-122. All FRHNs will have pre-provisioned DISN subscriber services via an initial request for service/telecommunications request/telecommunications order process coordinated through DISA. Any modifications or changes to the DISN subscriber services will be coordinated between the SC(T) and DISA using a request for service/telecommunications request/telecommunications order. The FRHN NOC will extend the DISN subscriber services to the deployed user. The following guidelines apply:

- Deployed users will request the extension of DISN services via an ASR submission.
- Deployed users will request changes to existing services via a change request (ASR) to the SC(T).
- In the event that user requests exceed the capacity of pre-positioned DISN subscriber services between the FRHN and DISA, the SC(T) may be required to submit a request for service/telecommunications request/telecommunications order to DISA to expand service capabilities.

MISSION FOLDER

I-123. The FRHN NOC will maintain a mission folder for each deployed customer (e.g., JNN-N enabled tactical unit). These folders are kept until one year after the circuit deactivates.

I-124. Each FRHN NOC will host a SIPRNET asynchronous collaboration portal server (e.g., Microsoft Sharepoint) with the following mission folder information:

- Mission/Exercise name.
- Dates/Times of mission/exercise.
- Mission priority.
- Operational satellite.
- Circuit types and data rates.
- Points of contact.
- Call sign of site and tactical terminal for out-of-band orderwire.
- SAR/ASR/ASA/SAA/telecommunications order/telecommunications request/request for service (Keep all revisions so changes and history can be tracked. Place the most current one on top for easy reference.)
- Mission diagrams, network topology provided by the deployed unit and other drawings. Place the electronic drawing in the circuit's folder under circuit actions, and print a copy for the physical folder.
- In-Effect/Completion/Exemption reports—keep all revisions.
- Delayed service reports—keep all revisions.
- Miscellaneous—all other related information includes:
    - Crew assignment sheets for the FRHN and each deployed customer.
    - COMSEC callout message.
    - ATO/IATO package for deployed unit—complete with statements of residual risk and consent to monitor/scan signed by the unit DAA.
    - ATC letter signed by the FRHN DAA.
    - After action review messages.
    - NETCOM/9th SC(A) NETOPS OPORD 05-01.
- Circuit priority and status matrix.
- Point of contact information for supported unit.

MISSION TRACKING AND STATUS REPORTS

I-125. Reporting will be conducted IAW OPORD 05-01. The SC(T) can supplement the reporting procedures to meet theater specific requirements.

MISSION PLANNING AND EXECUTION

I-126. Multiple organizations have a role in the planning and engineering for new missions landing at the FRHN. The ASCC will have overall oversight of the COMSEC layout supporting new missions. The ASCC will coordinate with the Joint COMSEC Management Office (controlling authority) to ensure keying material is compatible with JNN-equipped deploying units. The SC(T) will have overall FRHN planning and engineering responsibilities to include the identification of equipment strings (Tier 1 and Tier 2) and high-level device configuration (Tier 1). The FRHN NOC will have the responsibility for detailed device configuration (Tier 1) of VOIP, encryption, and private branch exchange; Tier 2 SATCOM and Promina configuration; operation and maintenance of the FRHN facility; and NOC operations for the FRHN. The TNOSC will have responsibility for detailed configuration of Tier 1 routers, IA devices, Army theater service desk, and develop SA views. The tactical unit will perform detailed device configuration for the remainder of Tier 2 equipment in the FRHN (e.g., routers, switches, VOIP, and encryption).

I-127. The ASCC will act as the COMSEC coordination point, while the SC(T) will:

- Coordinate mission planning with the deployed user and any other third party circuit providers as necessary.
- Conduct the planning and engineering for missions utilizing the FRHN.

- Develop ASA and disseminate to tactical unit and FRHN.
- Coordinate with the TNOSC to have Remedy ARS accounts created for the deployable force LNOs inside the FRHN NOC.
- Verify SAA and transmission plan with the tactical user and FRHN.
- Review COMSEC callout or intent to use message.
- Initiate wideband pre-access procedures.

I-128. The wideband pre-access process for the FRHN is dependent upon receipt of the SAA and transmission plan. During the wideband pre-access process, the following items must be confirmed by the SC(T):

- Satellite earth terminal is available and is in view of the assigned satellite.
- Availability of terminal equipment high power amplifier, low noise amplifier, up and down converters, and modems).
- Equipment can perform the mission (verify frequencies, capabilities of equipment, data rates, types of modulation, etc.).
- Verify commercial satellite vendor certification number (as required).
- Verify antenna polarization.
- Verify Host Nation approval, frequency clearance, landing rights and Federal Communications Commission licensing (as required).
- For cross-banding, ensure equipment requirements and availability.

I-129. The FRHN NOC will:

- Provide pre-defined "connectivity templates" to tactical units to streamline the requirements submission process. Connectivity templates are SAR and ASR templates that are tailored for specific types of units (e.g., division, BCT, ESB, etc.) to facilitate service request from the FRHN. The templates are tailored for each theater and made available on the FRHN portal server.
- Develop and implement equipment crew assignment sheets, including, but not limited to:
    - Private branch exchange configuration.
    - Tier 2 router and switch configuration—as requested by supported unit.
    - KIV-19 and KIV-7 configuration—per DISA standard configuration.
    - TACLANE KG-175 configuration.
    - Multiplexer Integration and Defense Communications Satellite Subsystem Automation System (MIDAS) configuration.
    - NET Promina Multiplexer configuration.
- Activate and troubleshoot circuits through the deployed user's lowest level multiplexer. The FRHN NOC is the controlling authority for the circuits extended to the deployed tactical user.
- Develop and disseminate reports IAW OPORD 05-01.
- Provide continuous (24 hour a day, 7 days a week, 365 days) operation and maintenance and expert assistance on mission and circuit activations through mission completion date (end of exercise [ENDEX]).
- Generate the COMSEC call out message.
- Ensure COMSEC updates Hotel Juliet are done daily or as required for on-going missions specified by the controlling authority (i.e., FRHN).
- Lead troubleshooting of SATCOM, VOIP, and legacy baseband (e.g., MIDAS, Promina, KGs, etc.)
- Ensure FRHN satellite contractor holds license to transmit/operate.
- Support LNOs with Tier 2 troubleshooting, as required.
- Provide Tier 2 configuration and management support in the absence of on-site LNOs or remote access from the deployed force.

- Report security incidents IAW Army and command procedures.
- Maintain operational CM of systems and devices in-use at the FRHN.
- Conduct real-time spectrum monitoring of the commercial TDMA and FDMA space segment.

I-130. The TNOSC will:

- Create Remedy ARS accounts for unit NETOPS cell personnel and LNOs located at the FRHN.
- Provide theater service desk support for the deployed force, FRHN, SC(T), and ASCC staff.
- Provide technical support for troubleshooting involving Tier 1 service support to the deployed forces.
- If requested from the unit, provide telephonic troubleshooting assistance with Tier 2 routing and IA issues.
- Develop NETOPS SA in support of theater NOSCs (e.g., tactical unit NOCs, JNCC, TNC, and TNCC) and the A-GNOSC.
- Configure and manage Tier 1 IA devices and routers in the FRHN.
- Have oversight of performance and health of the tactical Promina network that interfaces with the FRHN.
- Coordinate Tier 2 firewall access to supported units.
- Analyze IA sensor events throughout the deployed force network.

I-131. The supported tactical unit will:

- Submit the SAR, request for service, CST service survey, ASR, network diagram, and IATO/ATO to the ASCC.
- Collaborate with SC(T) engineers and FRHN technicians regarding requirements and equipment configuration.
- Verify accuracy and completeness of SAA and transmission plan.
- Review equipment crew assignment sheets for accuracy and ability to execute.
- Ensure COMSEC is on-hand at deployed locations.
- Operationally control Tier 2 equipment (less the SATCOM modems and Promina multiplexers). The unit is responsible for the configuration and management of the devices. The FRHN NOC retains the maintenance responsibility for the equipment.
- Identify and deploy LNOs to FRHN to configure and establish Tier 2 connectivity with their respective unit. Ideally, LNOs will remain onsite for the duration of the operation, and remain under the OPCON of their parent unit; however, the strategic signal brigade will provide administrative control support to the LNOs. The supported commander will determine manpower availability for LNOs deployed to the FRHN. It is feasible for the tactical unit to remotely administer their assigned Tier 2 devices in the FRHN.
- Provide the TNOSC and FRHN NOC access to information required to develop theater NETOPS shared SA.
- Implement equipment crew assignment sheets at deployed locations.
- Implement equipment crew assignment sheets for assigned Tier 2 equipment in the FRHN.
- Assist with troubleshooting communications connectivity with their assigned unit between their assets and the FRHN (with LNOs at the FRHN).
- Configure and manage assigned Tier 2 NETOPS packages in FRHN.
- Verify trouble tickets are input into the TNOSC service desk application.
- Coordinate with FRHN NOC for satellite access and baseband communications.
- Coordinate authorized service interruptions (ASIs) with TNOSC and FRHN NOC.
- Ensure that mission status and circuits are properly reported.
- Coordinate ENDEX with ASCC, SC(T), TNOSC, and FRHN NOC.
- Prepare and submit an after action report within 10 working days after end of access (format available at the FORSCOM G6 Spectrum Management AKO Knowledge portal

[AKO→Files→U.S. Army Organizations→FORSCOM→Knowledge Centers→G6 Spectrum Management])

NETWORK OPERATIONS REPORTING AND TROUBLESHOOTING PROCEDURES

I-132. For deployed force units that interface to the FRHN, NETOPS reporting will be conducted up through appropriate echelon NOSCs to the TNOSC. Deployed force units that are associated with a joint operation will report NETOPS data to a JNCC, with a lateral reporting responsibility to the TNOSC for SA. The deployed force units will provide the TNOSC access to information required to develop theater NETOPS shared SA for the JNN-N IP transport (i.e., VPN, Tier 1 routers, and Tier 2 routers). It should be noted that there is a lack of integration between deployable force and theater NETOPS systems, which complicates NETOPS reporting. The flow of NETOPS data is illustrated in Figure I-11.

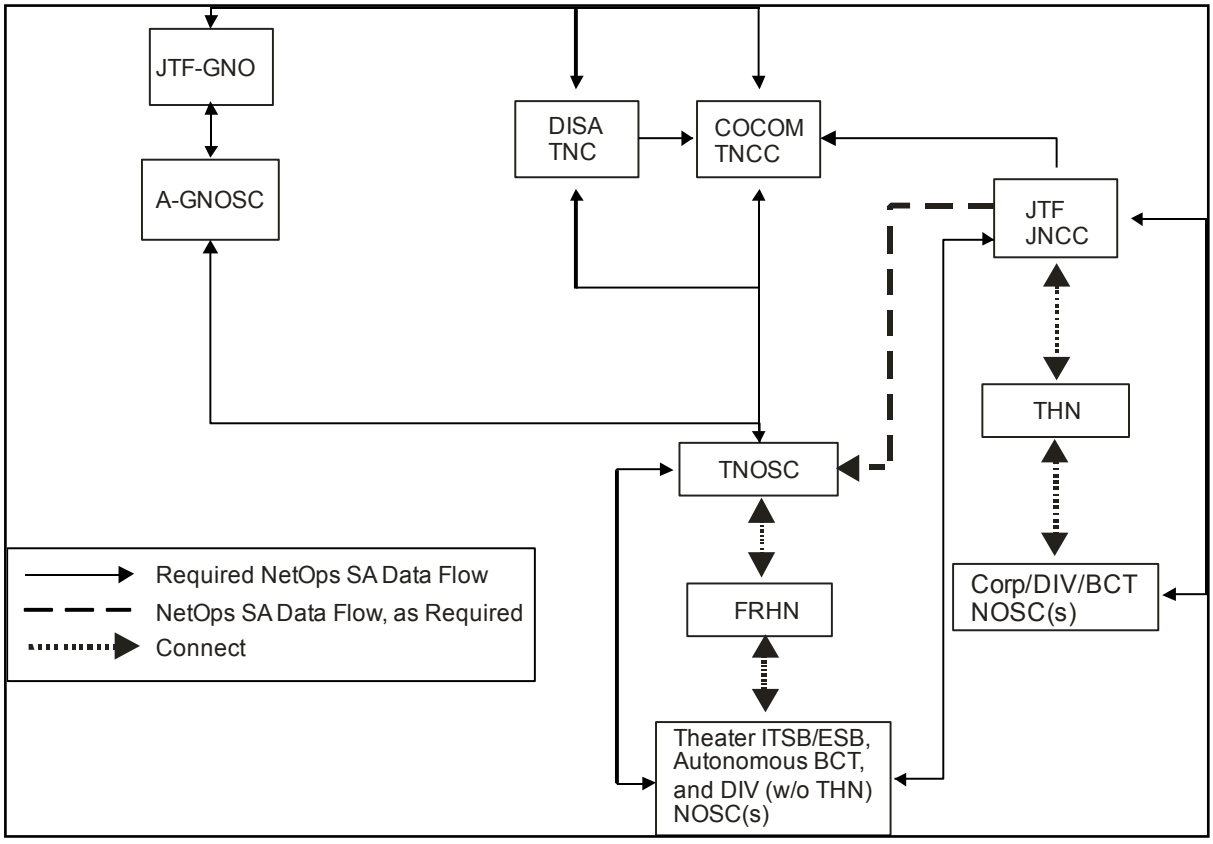

Figure I-11. Flow of NETOPS data

I-133. The FRHN NOC is notified of and/or identifies service degradation and outages and initiates the troubleshooting process. The FRHN NOC will determine the appropriate organization or entity to route the service calls to and initiate troubleshooting. See Figure I-12 for a high level diagram depicting the troubleshooting relationships.

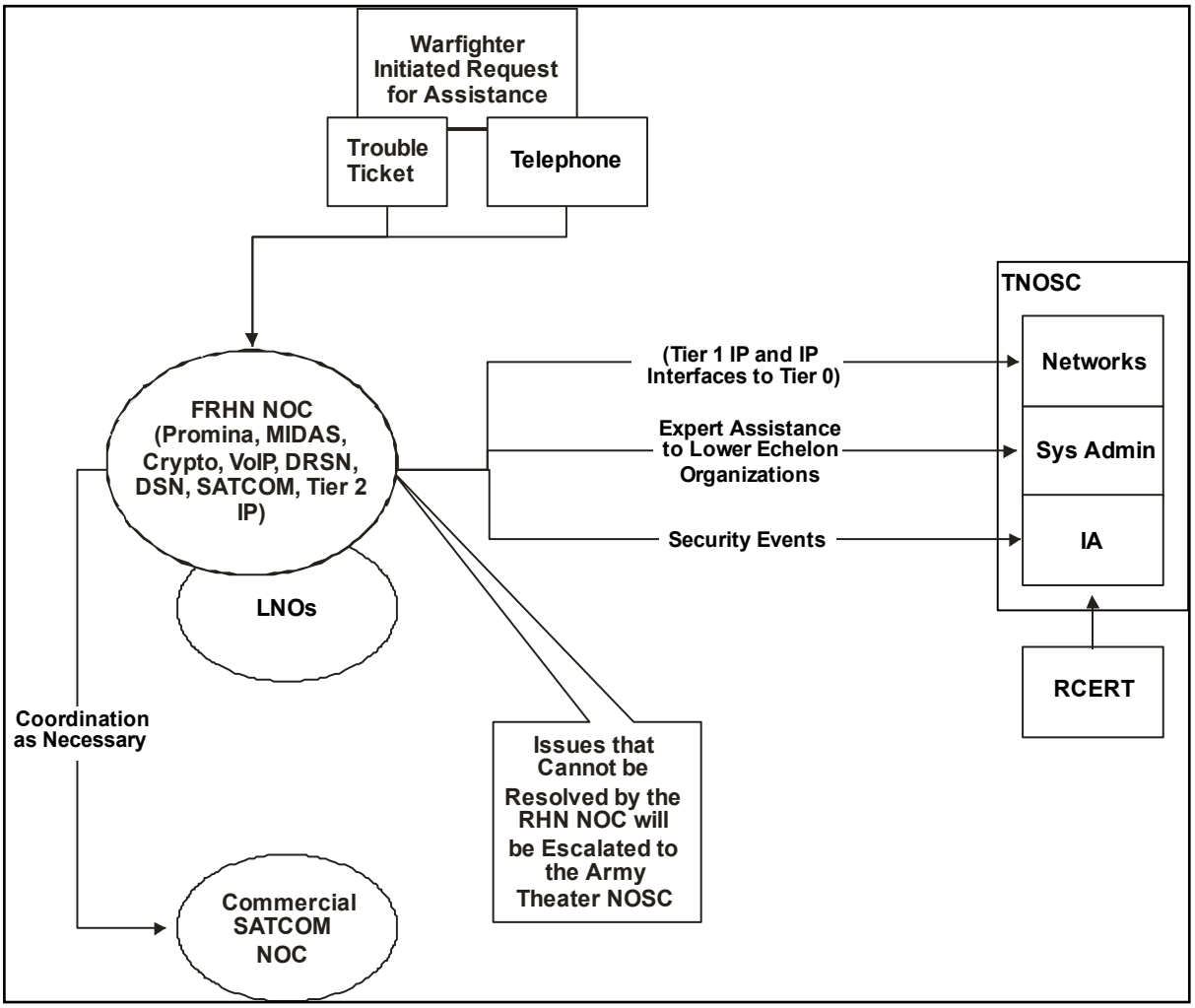

Figure I-12. Troubleshooting relationships

I-134. The FRHN NOC will:

- Be initial point of contact for FRHN NETOPS and troubleshooting issues.
- Initiate trouble tickets in support of the tactical units (as required).
- Escalate trouble tickets to TNOSC for theater level support (as required).
- Coordinate scheduled ASIs with the designated service desk no later than (NLT) 72 hours prior to outage (using Army theater service desk application).
- Coordinate emergency ASIs with the designated service desk NLT 24 hours (where possible) prior to the outage (using Army theater service desk application).
- Report unscheduled outages to the TNOSC IAW OPORD 05-01 (using TNOSC service desk application).
- Submit IA event reports (e.g., IAVM, incident/intrusions/virus, and data spillage, etc.) IAW AR 25-2 and Army Best Business Practices.
- Work with the TNOSC to close trouble tickets upon successful restoral (within 15 minutes of restoral).

I-135. The TNOSC will:

- Be the theater service desk for the deployed force.

- Set up reporting system to support FRHN and tactical formations (with A-GNOSC oversight).
- Set up NETOPS views.
- Set up and collect NETOPS SA data for the deployed force and disseminate to tactical NOCs, JNCCs, CCDR TNCC, DISA TNC, and the A-GNOSC per existing SOP.
- Create custom SA views to support joint theater level NOSCs.

I-136. The unit will:

- Report scheduled ASIs affecting the WAN transport to the FRHN NOC NLT 72 hours prior to the outage (via telephonic or electronic means [Army theater service desk application]).
- Report emergency ASIs affecting the WAN transport to the FRHN NOC NLT 24 hours (where possible) prior to the outage (via telephonic or electronic means [Army theater service desk application]).
- Report unscheduled outages to the FRHN NOC IAW OPORD 05-01 (via telephonic [in-band or out-of-band] or electronic means [Army theater service desk application]).
- Work with FRHN NOC to close trouble tickets upon successful service restoral.
- Submit IA event reports (e.g., IAVM, incident/intrusions/virus, and data spillage, etc.) IAW AR 25-2 and Army Best Business Practices.
- Interface and report to the JNCC per JTF requirements.

I-137. In the near-term, there is a disparity in the NETOPS applications that have been fielded to JNN-N equipped units and the TNOSCs/A-GNOSC. The FRHN is fielded with JNN-N compatible applications, and will aggregate NETOPS data from the deployed forces with which it interfaces. FRHN NETOPS data will be interfaced with the TNOSC to develop SA views for lateral and vertical consumers.

ACCESS PROCEDURES

I-138. The following paragraphs discuss access procedures.

WIDEBAND ACCESS PROCEDURES

I-139. The following is guidance for the FRHN on satellite access:

- Deployed user calls FRHN NOC using out of band communications (e.g., cell phone, Iridium, international maritime satellite, etc.) and indicates they are ready to access the satellite.
- FRHN NOC has assigned FDMA and TDMA carriers online awaiting deployed force access.
- Deployed user acquires FDMA or TDMA receive carrier(s) and adjusts azimuth/elevation and polarization to maximize receive signal.
- Deployed user calls FRHN NOC, using out-of-band communications, and indicates ready to begin transmitting.
- FRHN NOC initiates conference call to include deployed force user and DISN Satellite Transmission System-Global NOC.
- DISN Satellite Transmission System-Global hub operator works with deployed force user to fine tune polarization and adjust transmit power.

BASEBAND ACCESS PROCEDURES

I-140. The FRHN NOC is the controlling authority for the activation of all circuits as well as troubleshooting, etc. The following information is a high-level example of baseband access procedures. More detailed information will be contained in tactics, techniques, and procedures and SOPs, which will be available on the FRHN SIPRNET portal servers. Other procedures include:

- Once the FRHN FDMA carrier is on the satellite, the operator shall confirm by bit error rate test via transmit satellite loopback. In certain cases, this will be impossible to do because of satellite antenna configuration, etc. The FRHN operator shall also normalize the receive frequency on the down converter and then qualify the link by running the bit error rate test for 30 minutes (period

can be shortened or testing terminated, depending on coordination between the commercial satellite NOC, the FRHN, and the JNN-N enabled tactical user) end to end with the JNN-N enabled tactical user's Firebird, preferably between the Red side of the FRHNs crypto device and the JNN-N enabled tactical user's crypto device. Some units lack Firebird equipment, so a loopback at the tactical end back towards the gateway should be performed to confirm connectivity, again at to the lowest level possible). This provides validation that the radio frequencies are correct, the modem settings are correct, the crypto device strappings are compatible, and the correct COMSEC segment is being used. A multiplexer loopback can be extended to include the Promina SA-TRK card. The Promina will indicate green up with a downloop condition on the SA-TRK card. This quickly verifies the path and all equipment in the string at that point through the satellite.

- After the link has been qualified, the FRHN operator shall normalize both sides to connect the multiplexers end-to-end. The multiplexers should lock up. After the SA-TRKs are working, the individual circuits can then be programmed and/or mapped.
- If there is adequate bandwidth in the overall aggregate, a permanent test circuit should be provisioned.
- FRHN personnel will work with the deployed units to establish DSN trunks, DRSN trunks, and the IP subsystems.

CONFIGURATION MANAGEMENT PROCEDURES

I-141. The program manager for DCATS will maintain physical plant CM of rack face elevations, hardware, software version, and firmware version control for equipment in the FRHNs. Coordination between the program manager, DCATS; the program manager, tactical radio communications systems; SC(T); FRHN NOC; and the TNOSC will be necessary to ensure accuracy of the CM database. The program manager, DCATS, will disseminate software and firmware updates and hardware modifications to the appropriate organizations for coordination and activation. The program manager, DCATS, will test all updates/modifications prior to dissemination to the field. Figure I-13 is a high level diagram illustrating the concept.

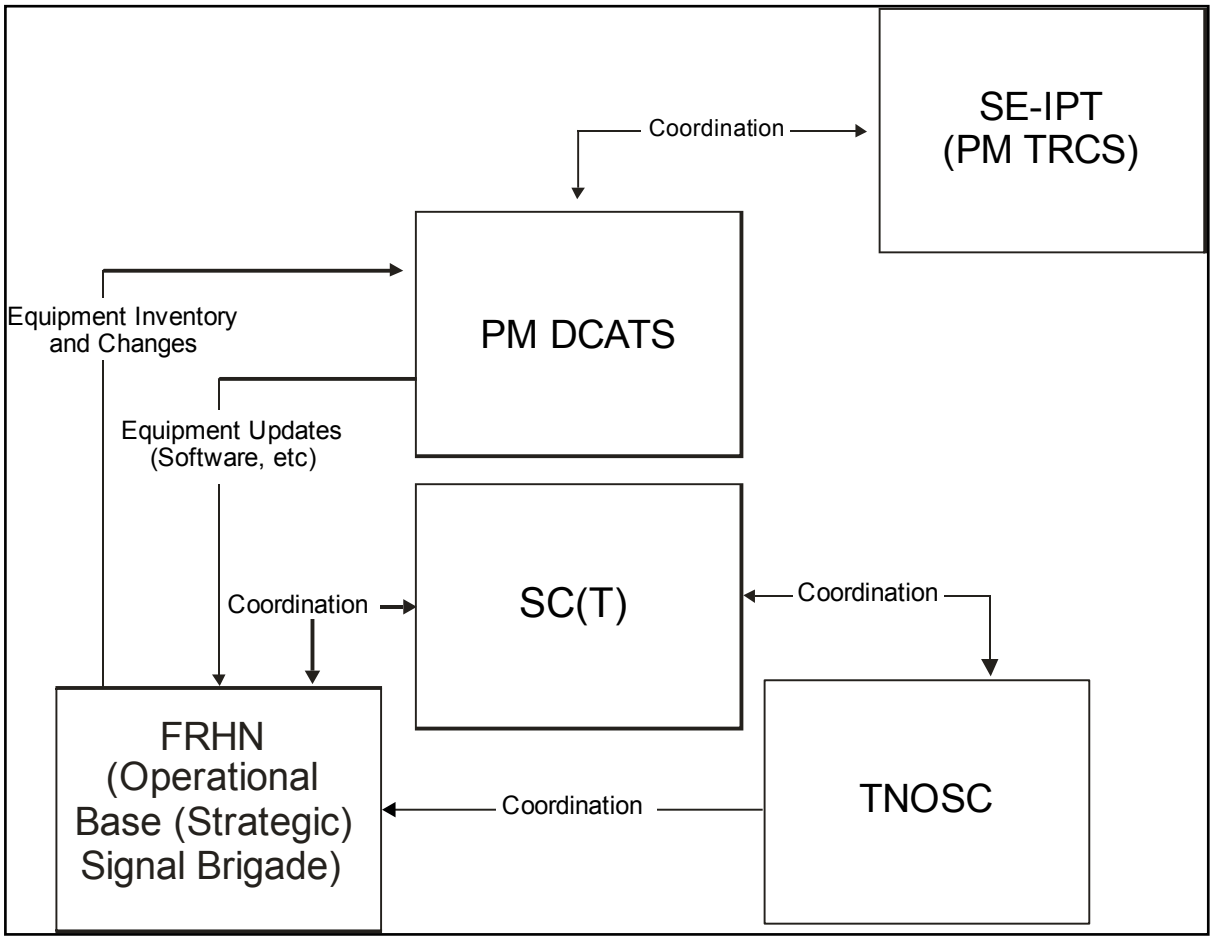

Figure I-13. Physical plant configuration management flowchart

I-142. Initially, operational CM information will be contained in a spreadsheet format. In the future, CM is envisioned to be tracked and contained in a configuration management database (CMDB) system. The CMDB may or may not be co-located with the FRHN; however, FRHN, TNOSC, and SC(T) personnel will have access to the system. Figure I-14 is a high-level description of the operational CM process.

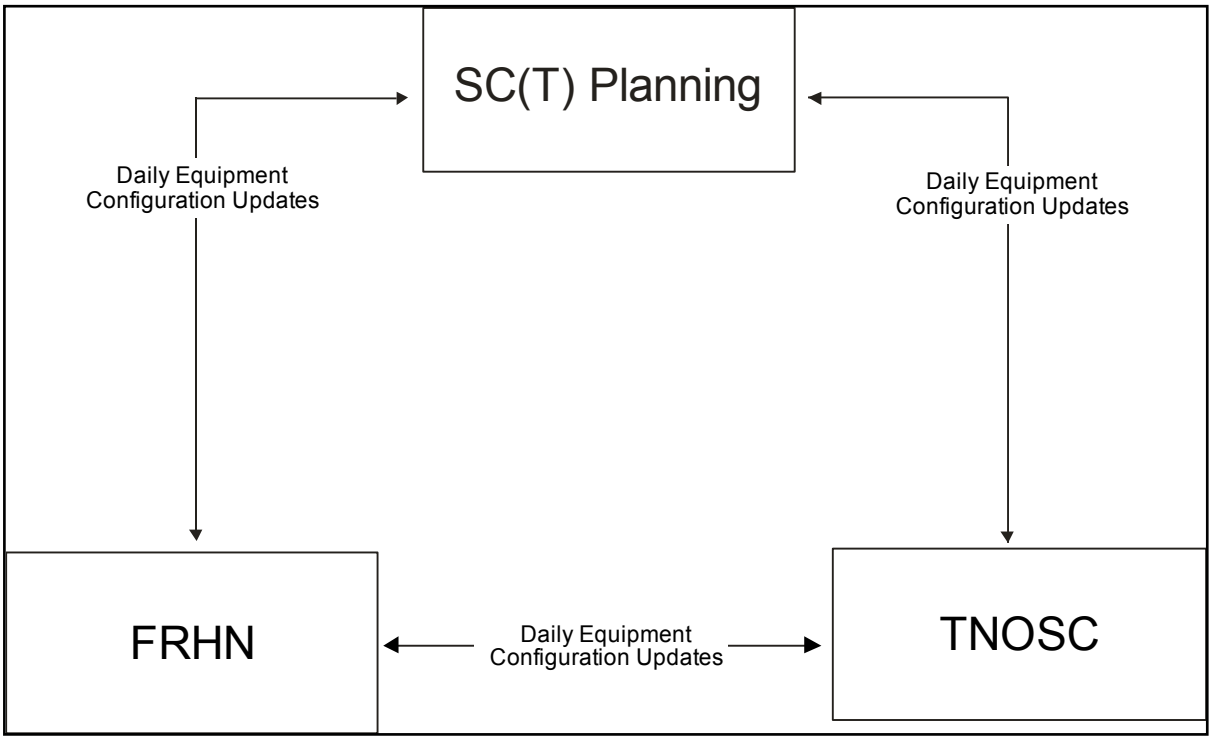

Figure I-14. Operational configuration management process

FAILOVER FROM A TACTICAL HUB NODE TO A FIXED REGIONAL HUB NODE

I-143. Two failover options are available. One failover option is to preposition tactical unit configuration information at the FRHN NOC, and perform a manual cutover at the direction of the tactical commander. This option will likely take several hours to execute and bring the tactical unit up on the FRHN.

I-144. The second failover option is to have the FRHN participate in the supported unit's TDMA meshes at all times. If the THN becomes inoperable, the NCC in the FRHN NOC will be brought online to control the mesh. This option provides the fastest failover capability for the TDMA network. FDMA circuits will still require a manual cutover. Development of a technical solution to this failover option is being pursued by the Systems Engineering Integrated Product Team.

I-145. If a failover is necessary and FRHN resources are unavailable, the ASCC (ICW the CCDR) will adjudicate mission priorities. Ideally, initial priorities should be established as part of the mission planning process.

I-146. The following factors will have to be considered to execute a failover:

- Is the FRHN in the same satellite coverage area as the THN? This may require transfer of mission(s) to new satellite.
- What is the current command relationship specifically as it pertains to the THNs division commander and the FRHN's SC(T) commander? The direction could come from the ASCC or the CCDR or both depending on the environment.
- Are transmission plans and link budgets pre-positioned?
- Are frequency clearances for FRHN pre-positioned?
- Is authority to transmit for FRHN pre-positioned?
- Is synchronization of the network and reroute plan available?

CONTINUITY OF OPERATIONS

I-147. COOP capability between FRHNs would be a manual process. Figure I-15 depicts the relationships and information gaps that would require full synchronization for immediate COOP capability between FRHNs.

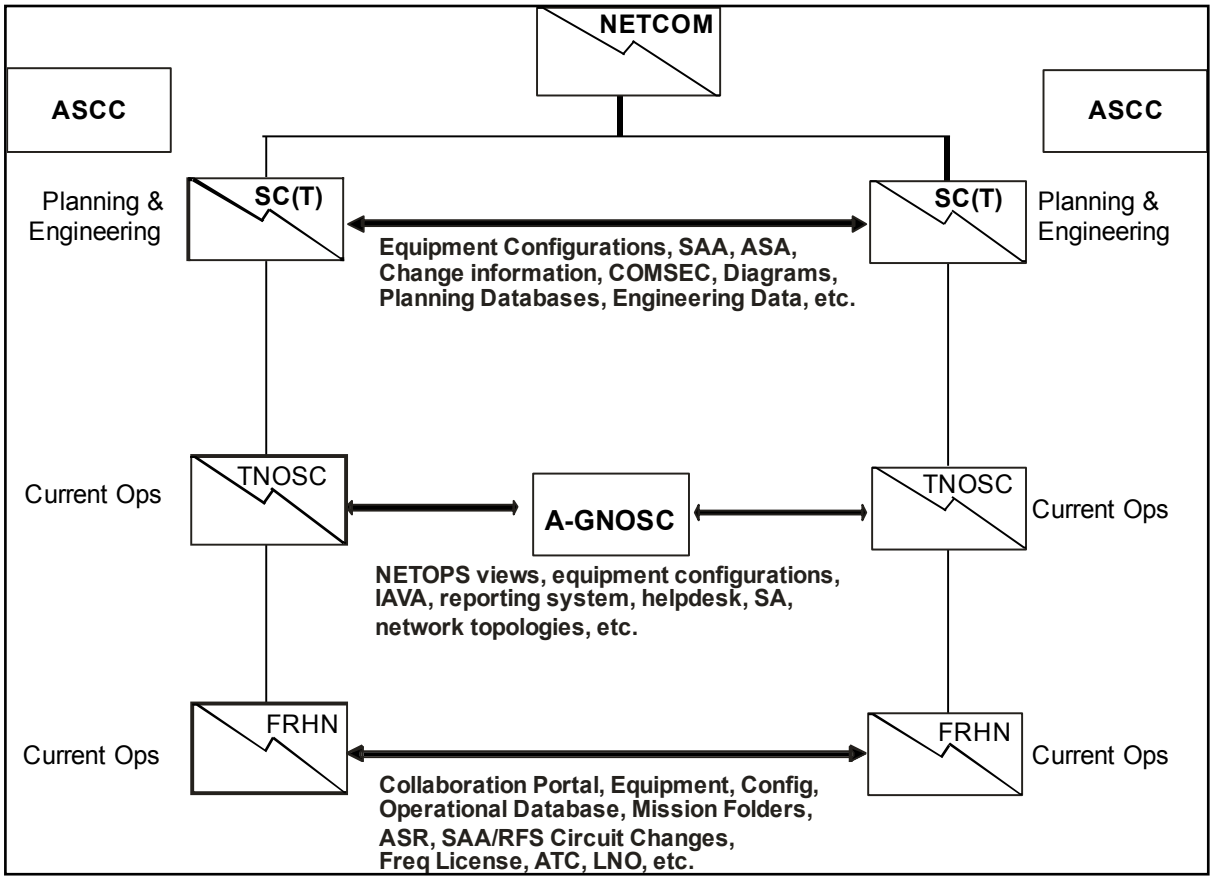

Figure I-15. COOP precursors

END OF EXERCISE PROCEDURES

I-148. The unit identifies the Start of Exercise, or mission, and ENDEX times in the SAR/ASR submission. Prior to communications termination, the unit will coordinate with the TNOSC service desk 24 hours prior to communications termination, and again 30 minutes prior to communications termination.

I-149. If the ENDEX time/date is different than what is identified in the SAR/ASR, a formal record message shall be sent by the unit to the ASCC identifying the point of contact details, original SAR/ASR ENDEX date time group, requested new ENDEX date time group, and the purpose for extension or early termination. It is imperative that the message for an extension be sent as early as possible to ensure space segment is available and leased to support the duration of the mission.

I-150. The unit will submit an after action review within 10 days of ENDEX to the ASCC and SC(T). Once the after action review has been disseminated, the TNOSC will post an electronic copy in the mission planning folder. The after action review will be in Microsoft Word or Adobe Acrobat format. The after action review should be used to identify processes and procedures that worked well and/or need improvement. Recommendations to improve the processes and procedures are encouraged. Recommended categories include:

- Service request process (e.g., SAR/ASR/CST service survey and validation/adjudication).
- Planning and engineering process which includes:
    - Collaborative planning process involving the unit, SC(T), FRHN NOC, TNOSC, and CCDR J-6.
    - Detail and accuracy of equipment crew assignment sheets.
- Service acquisition process for:
    - SATCOM.
    - Baseband.
- TNOSC categories:
    - Service delivery.
    - Reporting.
    - Troubleshooting.
    - Responsiveness.

FIXED REGIONAL HUB NODE TRAINING

I-151. The FRHN personnel will receive new equipment training by the fielding agency. The FRHN leadership will capitalize on the provided training materials and set up an in-house sustainment training program to be taught by personnel organic to the organization. Training will be incorporated into the unit's mission essential task list. The training program will:

- Cover all equipment operations, maintenance, management, and administration tasks.
- Provide a matrix/planning schedule that ensures that all training tasks are trained at least annually.
- Identify all training skill level shortcomings.
- Provide a training assessment of site personnel and the site overall.
- Schedule, conduct, and document any additional or supplemental training, as required.
- Make training records available for review during command inspections, performance evaluations, etc.

Glossary

The glossary lists acronyms and terms with Army, multi-service, or joint definitions, and other selected terms. Where Army and joint definitions are different, (Army) follows the term. Terms for which FM 6-02.71 is the proponent manual (the authority) are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

A2C2S	Army Airborne Command and Control System
A2TOC	Army Global Network Operations and Security Center and Army Computer Emergency Response Team Tactical Operations Center
A&VTR	Army asset and vulnerability tracking resource
ABCS	Army Battle Command System
ACERT	Army computer emergency response team
ACES	Automated Communications Engineering Software
ACL	access control list
ACOM	Army Command
AD	active directory
ADCON	administrative control
AEI	Army Enterprise Infrastructure
AENIA	Army enterprise network operations integrated architecture
A-GNOSC	Army global network operations and security center
AIAP	Army Information Assurance Program
AKO	Army Knowledge Online
AOR	area of responsibility
APC	area processing centers
AR	Army regulation
ARFOR	Army forces
ARSTRAT	United States Army Forces Strategic Command
ASA	Army service authorization
ASAS	All Source Analysis System
ASCC	Army Service component command
ASI	authorized service interruption
ASR	Army Service Request
ATC	authority to connect
ATM	asynchronous transfer mode
ATO	authority to operate
BCT	brigade combat team
bde	brigade
BFSB	battlefield surveillance brigade
BFT	Blue Force Tracking

bn	battalion
BOIP	basis of issue plan
BPMN	business process modeling notation
C2	command and control
CC/S/A	combatant commands, services, and agencies
CCB	configuration control board
CCDR	combatant commander
CDRUSSTRATCOM	Commander, United States Strategic Command
CENTCOM	Central Command
CERT	computer emergency response team
CG	Commanding General
CI	configuration item
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CJTF	commander, joint task force
CJTF-GNO	commander, joint task force-global network operations
CM	configuration management
CMD	command
CMDB	configuration management database
CND	computer network defense
COA	course of action
COCOM	combatant command (command authority)
COMSEC	communications security
CONOPS	concept of operations
CONUS	continental United States
COOP	continuity of operations
CP	command post
CPN	command post node
CS	content staging
CSS	combat service support
CST	commercial satellite team
DAA	designated approval authority
DET	detachment
DCATS	Defense Communications and Army Transmissions System
DHCP	dynamic host configuration protocol
DID	defense in depth
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process

DIMHRS	Defense Integrated Military Human Resources System
DIRLAUTH	Direct Liaison Authorized
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
div	Division
DMAIN	division main
DMZ	demilitarized zone
DNS	domain name service
DOD	Department of Defense
DOD-CERT	Department of Defense Computer Emergency Response Team
DOIM	directorate of information management
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DTAC	division tactical command post
EHF	extremely high frequency
EIS	Enterprise Information Systems
e-mail	electronic-mail
ENDEX	end of exercise
ENM	Enhanced Position Location Reporting System network manager
EPLRS	Enhanced Position Location Reporting System
ERP	Enterprise Resource Planning
ESB	expeditionary signal battalion
ESM	enterprise systems management
EUCOM	European Command
EUSA	Eighth United States Army
EKMS	Electronic Key Management System
FBCB2	Force XXI Battle Command, Brigade and Below
FCC	functional component commander
FDMA	frequency division multiple access
FM	field manual
FMI	field manual interim
FORSCOM	United States Army Forces Command
FRAGO	fragmentary order
FRHN	fixed regional hub node
FTP	File Transfer Protocol
G-1	assistant chief of staff, personnel
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-6	assistant chief of staff, command, control, communications, and computer

	operations
G-7	assistant chief of staff, information operations
GAR	gateway access request
GBS	Global Broadcast Service
GCC	geographic combatant commander
GCM	Global Information Grid content management
GEM	Global Information Grid enterprise management
GIG	Global Information Grid
GISMC	Global Infrastructure Service Management Center
GMF	ground mobile forces
GNC	global network operations center
GNCC	global network operations control center
GND	Global Information Grid network defense
GNO	global network operations
GNOSC	global network operations and security center
GNSC	global network operations support center
GSALT	global command and control system administration log tool
GSSC	global satellite communications support center
HCLOS	high capacity line of sight
HQ	headquarters
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HSOC	homeland security operations center
IA	information assurance
IAM	information assurance manager
IANM	information assurance network manager
IANO	information assurance network operator
IAPM	information assurance program manager
IASO	information assurance security officer
IATO	interim authority to operate
IAVA	information assurance vulnerability alert
IAVB	information assurance vulnerability bulletin
IAVM	information assurance vulnerability management
IAW	in accordance with
IC-IRC	Intelligence Community-Incident ResponseCenter
ICW	in coordination with
ID	infantry division
IDM	information dissemination management
IDM-T	information dissemination management-tactical
IDS	intrusion detection system

IMCEN	information management center
INFOCON	information operations condition
INMARSAT	international maritime satellite
IO	information operations
IOC	initial operational capability
IO CMD	information operations command
IP	Internet Protocol
IPS	intrusion prevention system
ISDN	Integrated Services Digital Network
ISYSCON	integrated systems control
IT	information technology
ITSB	integrated theater signal battalion
J-2	intelligence directorate of a joint staff; intelligence staff section
J-6	communications system directorate of a joint staff; command, control, communications, and computer systems staff section
JFCC-NW	Joint Functional Component Command Network Warfare
JFLCC	joint force land component commander
JNCC	joint network operations control center
JNN	joint network node
JNN-N	joint network node-network
JNTC	Joint Network Transport Capability
JP	joint publication
JTA-A	joint technical architecture-Army
JTF	joint task force
JTF-GNO	joint task force-global network operations
JTRS	joint tactical radio system
JTSSNMCCB	Joint Tactical Switched Systems Network Management Configuration Control Board
LAN	local area network
LIAA	LandWarNet information assurance architecture
LNO	liaison officer
LCMS	Local COMSEC Management Software
LMD/KP	Local Management Device /Key Processor
LOS	line of sight
Log-Net	Logistics-Network
LWN	LandWarNet
MBCOTM	mounted battle command on the move
MBITR	multiband inter/intra team radio
Mbps	megabits per second
MEDCOM	United States Army Medical Command

MIDAS	Multiplexer Integration and Defense Communications Satellite Subsystem Automation System
MRHN	mobile regional hub node
MSS	Mobile satellite service
MTSS	military training service support
NCC	network control center
NET	network
NETCOM	Network Enterprise Technology Command
NETOPS	network operations
NIDS	network intrusion detection system
NIPR	Non-Secure Internet Protocol Router
NIPRNET	Non-Secure Internet Protocol Router Network
NLT	no later than
NM	network management
NOC	network operations center
NORTHCOM	Northern Command
NOSC	network operations and security center
O&M	operations and maintenance
OCONUS	outside the continental United States
OIF/OEF	Operation Iraqi Freedom/Operation Enduring Freedom
OPCON	operational control
OPORD	operation order
OPSEC	operations security
PACOM	Pacific Command
PBX	private branch exchange
PEO	program executive office
PKE	public key enabled
PKI	public key infrastructure
PM	program manager
PM DCATS	Program Manager-Defense Communications and Army Transmissions System
RADIUS	remote authentication dial-in user server
RCERT	regional computer emergency response team
RCIO	regional chief information officer
RFS	request for service
RHN	regional hub node
RNOSC	regional network operations and security center
RSSC	regional satellite support center
S-2	intelligence staff officer
S-3	operations staff officer
S-6	command, control, communications, and computer operations

SA	situational awareness
SAA	satellite access authorization
SAR	satellite access request
SATCOM	satellite communications
SBDE	support brigade
SB(T)	signal brigade (tactical)
SC(A)	signal command (Army)
SC(T)	signal command (theater)
SECDEF	Secretary of Defense
SGNOSC	service global network operations and security center
SIGOPS	signal operations
SINCGARS	single-channel ground and airborne radio system
SIPR	SECRET Internet Protocol Router
SIPRNET	SECRET Internet Protocol Router Network
SLA	service level agreement
SMART-T	Secure Mobile Antijam Reliable Tactical Terminal
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	standing operating procedure
SOUTHCOM	Southern Command
SSIO	system integration oversight
STB	special troops battalion
STEP	standard tactical entry point
STIG	security technical implementation guide
STNOSC	Service theater network operations and security center
SVCS	services
TAC	tactical
TACLANE	tactical local area network encryptor
TACON	tactical control
TDMA	time division multiple access
THN	tactical hub node
THSDN	tactical high speed data network
TIC	tactical integration cell
TJTNCCB	Theater Joint Tactical Network Configuration Control Board
TLT	tactical liaison team
TNC	theater network operations center
TNCC	theater network operations control center
TNOSC	theater network operations and security center
TNT	tactical network team
TOC	tactical operations center

TP	Transmission plan
TRADOC	United States Army Training and Doctrine Command
TRCS	tactical radio communications systems
Trojan SPIRIT	Trojan special purpose integrated remote intelligence terminal
TSO	telecommunications service order
TS/SCI	top secret/sensitive compartmented information
UHF	ultrahigh frequency
UHN	unit hub node
US	United States
USARCENT	United States Army, Central
USAREUR	United States Army, Europe
USARPAC	United States Army, Pacific
USASC&FG	United States Army Signal Center and Fort Gordon
USARSO	United Stated Army, South
USASMDC	United States Army Space and Missile Defense Command
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USSTRATCOM	United States Strategic Command
VOIP	Voice over Internet Protocol
VPN	virtual private network
WAN	wide area network
WATCHCON	watch condition
WIN-T	Warfighter Information Network-Tactical
WISC	warfighter integration and support cell

SECTION II – TERMS

ARFOR

(Army) The senior Army headquarters and all Army forces assigned or attached to a combatant command, subordinate joint force command, joint functional command, or multinational command. (FM 3-0)

combatant command (command authority)

(joint) Nontransferable command authority established by Title 10 (“Armed Forces”), United States Code, Section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces,

assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). (JP 1-02)

computer network defense

(joint) Actions taken through computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 6-0)

Global Information Grid

(joint) The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information in demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 6-0)

information assurance

(joint) Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-13)

information superiority

(joint) The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 3-13)

***LandWarNet**

The Army's portion of the GIG.

local area network

A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. Note 1: LANs are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. Note 2: An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network. An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network. Note 3: LANs are not subject to public telecommunications regulations. (Federal Standard 1037C)

metropolitan area network

A data communications network that (a) covers an area larger than a campus area network and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs. (Federal Standard 1037C)

network operations

(joint) Activities conducted to operate and defend the Global Information Grid. (JP 6-0)

operational control

(joint) Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority)

and may be delegated within the command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish the missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. (JP 1-02)

tactical control

(DOD) Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (JP 1-02)

***technical channels**

Technical channels provides commanders with the means to rapidly employ or modify functional capabilities for mission requirements. It enables the timely implementation of techniques, procedures, standards, configurations, and designs in support of operations at all levels. Technical channels neither constitutes nor bypasses command authority, but serves as the mechanism for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of full spectrum operations. The orders process will delineate the appropriate authorities required to implement functional capabilities from Army down to the lowest echelons of command through the use of technical channels.

wide area network

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks, X.25 networks, and T1 networks. Note 2: A metropolitan area network is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide. (Federal Standard 1037C)

Wireless Personal Area Network

A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either RF (e.g., Bluetooth) or IR technology. (DOD Directive 8100.2)

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

ARMY PUBLICATIONS

AR 10-87. *Army Commands, Army Service Component Commands, and Direct Reporting Units*. 04 September 2007.

AR 25-1. *Army Knowledge Management and Information Technology*. 15 July 2005.

AR 25-2. *Information Assurance*. 24 October 2007.

AR 25-6. *Military Affiliate Radio System (Mars) and Amateur Radio Program.* 01 May 2007.

AR 380-5. *Department of the Army Information Security Program.* 29 September 2000.

AR 380-40. *Policy for Safeguarding and Controlling Communications Security (COMSEC) Materiel*. 30 June 2000.

AR 380-53. *Information Systems Security Monitoring*. 29 April 1998.

AR 500-3. *U.S. Army Continuity of Operations (COOP) Program Policy and Planning.* 12 April 2006.

Bronson, J. and Knight, L. CIO/G6 White Paper v6.5. *Army's Adjusted Teleport Gen II Satellite Communications (SATCOM) Circuit-switched and Internet Protocol (IP) Requirements*. 11 August 2006.

FM 3-0. *Operations*. 27 February 2008.

FM 3-13. *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* 28 November 2003.

FM 3-21.21. *The Stryker Brigade Combat Team Infantry Battalion*. 8 April 2003.

FM 5-19. *Composite Risk Management.* 21 August 2006.

FM 6-0. *Mission Command: Command and Control of Army Forces.* 11 August 2003.

FMI 5-0.1. *The Operations Process (with change 1).* 31 March 2006.

FMI 6-02.45. *Signal Support to Theater Operations.* 05 July 2007.

FMI 6-02.60. *Tactics, Techniques, and Procedures (TTPs) for the Joint Network Node-Network (JNN-N)*. 05 September 2006.

FMI 6-02.70. *Army Electromagnetic Spectrum Management Operations.* 05 September 2006.

NETCOM. *Fixed Regional Hub Node (FRHN) Operations and Control (O&C) Plan. Version 1.3.* 17 July 2007

Technical Bulletin 380-41. *Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material.* 16 June 2006. (Current as of 16 June 2006.)

US Army Chief Information Officer/G-6. *Army Network Operations Concept of Operations (version 1.0)*.

US Army Chief Information Officer/G-6 Policy Memorandum. *Enterprise Network Operations Integrated Architecture Implementation.* 24 April 06.

US Army Chief Information Officer/G-6 White Paper. *Fight the Network*. 08 September 2004.

US Army Office of Information Assurance and Compliance. *Army Password Standards. Version 2.5.* 1 MAY 08

JOINT PUBLICATIONS

Chairman of the Joint Chiefs of Staff, Director for Strategic Plans and Policy, J-5, Strategy Division. *Joint Vision 2020.* September 2000.

CJCSI 6211.02B. *Defense Information System Network: Policy, Responsibilities and Processes.* 31 July 2003.

CJCSI 6215.01C. *Policy for Department of Defense Voice Networks with Real Time Service.* 09 November 2007.

CJCSI 6510.01E. *Information Assurance (IA) and Computer Network Defense (CND.* 15 August 2007

CJCSM 6231.01C. *Manual for Employing Joint Tactical Communications Joint Systems Management.* 21 June 2007.

CJCSM 6231.07D. *Manual for Employment of Joint Tactical Communications-Joint Network Management and Control*. 24 October 2007.

CJCSM 6510.01. *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND).* 14 March 2007.

Defense Information Systems Agency (DISA). *Global Contingency and Exercise Planning (CONEX) Guide*. January 2003.

Department of the Army Pamphlet 25-1-2. *Information Technology Contingency Planning*. 16 November 2006.

Department of Defense Directive 8100.02. *Use Of Commercial Wireless Devices, Services, And Technologies In The Department Of Defense (DOD) Global Information Grid (GIG).* 14 April 2004.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 12 April 2001.

JP 3-0. *Joint Operations.* 17 September 2006.

JP 3-13. *Information Operations.*13 February 2006.

JP 5-0. *Joint Operation Planning.* 26 December 2006.

JP 6-0. *Joint Communications System.* 20 March 2006.

Strategic Command Directive (SD) 527-1. *DOD Information Operations Condition (INFOCON) System Procedures*. 27 January 2006.

United States Strategic Command. *Joint Concept of Operations for Global Information Grid NetOps.* 04 August 2006.

United States*. Unified Command Plan 2002.*

United States. *Unified Command Plan 2004. March 2005*

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

DA Form 2028. *Recommended Changes to Publications and Blank Forms.* February 1974.

Business Process Modeling Notation (version 1.0 specification). May 2004.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

CJCSM 3122.01A. *Joint Operation Planning and Execution System (JOPES.,* Volume I. 29 September 2006.

CJCSM 3122.03B. *Joint Operation Planning and Execution System (JOPES.,* Volume II. 28 February 2006.

CJCSM 3150.16A. *Joint Operation Planning and Execution System Reporting Structure (JOPESREP)*. 29 September 2000.

CJCSM 3320.01B. *Joint Operations in the Electromagnetic Battlespace.* 25 March 2006.

Department of Defense. *NetCentric Joint Functional Concept.* 7 April 2005.

Department of Defense. *Transformational Communications Architecture Concept of Operations (CONOPS).* 28 February 2003.

FM 3-07. *Stability Operations and Support Operations.* 20 February 2003.

FM 3-07.31. *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations.* 26 October 2003.

FM 3-31. *Joint Force Land Component Commander Handbook (JFLCC)*. 13 December 2001.

FM 4-01.011. *Unit Movement Operations.* 31 October 2002.

US Army Training and Doctrine Command, Task Force Modularity. *Army Comprehensive Guide to Modularity.* 08 October 2004.

Index

1

D

E

1